La protection des données dans l'Espace européen de liberté, de sécurité et de justice

JOURET, J.; MOREAU, D.; Dumortier, Franck; Gayrel, Claire; Poullet, Yves

Published in:
Journal de droit européen

Publication date:
2010

Document Version
le PDF de l'éditeur

Journal de droit européen

Février 2010
N° 166 — 18e année

Bureau de dépôt : Louvain 1 - Mensuel, sauf juillet/août

larcier

ISSN 0779-7656 – D 2010/0031/039

Paul NIHOUL, rédacteur en chef

ANALYSE

La protection des données dans l'Espace européen de liberté, de sécurité et de justice

L'APPLICATION DES RÈGLES EUROPÉENNES *sur la protection des données aux questions concernant l'Espace européen de liberté, de sécurité et de justice conduit-elle à un renforcement des principes consacrés par ces règles, ou au contraire, à leur affaiblissement ?*

1 Introduction

Ces dernières années se sont multipliées les initiatives de l'Union européenne liées tant à la sécurité nationale, en ce compris la lutte contre l'immigration illégale, qu'à la recherche d'infractions. La révélation par la STOA[1] des agissements du réseau Echelon[2], vaste système de surveillance satellitaire mis au point par les services secrets notamment américains et anglais ont fait craindre pour nos souverainetés nationales et ont suscité, quelques jours avant les événements dramatiques du 11 septembre 2001, des réactions virulentes du Parlement européen[3] fondées notamment sur l'exigence d'un respect hors frontières des principes de la protection des données. La tendance dite sécuritaire qui s'est manifestée partout en Europe suite aux attentats de New York, Londres et Madrid, a largement débordé le cadre de la lutte antiterroriste[4] et a conduit à un renforcement des coopérations policières et judiciaires dans l'Union européenne. Ainsi, des textes nombreux ont été proposés voire adoptés en matière de lutte antiterrorisme. De plus, les transferts d'information entre les administrations chargées des contrôles aux frontières dans le cadre de CIS (Customs information System)[5], VIS (Visa Information System)[6], Schengen I et II[7] et entre les autorités policières et judiciaires dans le

(1) Le STOA (Advisory Committee of the EU Parliament on Technology Assessment) publia différents rapports à propos du système de surveillance Echelon fondés sur les révélations de journalistes tels J. Bamford, « The puzzle Palace » ou N. Hager, « The Secret power », en particulier « Development of surveillance Technology and Risk of abuse of economic information », Luxembourg, mai 1999.

(2) À propos de ce réseau d'écoute des messages transitant par des satellites, D. Yernault, « L'efficacité de la Convention européenne des droits de l'homme pour contester le système "Echelon" », *in* Sénat et Chambre des représentants de Belgique, « Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé "Echelon" », 25 février 2002.

(3) Résolution du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système « Échelon ») du 5 septembre 2001, *J.O.C.E.* C 072 E, 21 mars 2002, pp. 0221-0229.

(4) Sur la difficulté d'une définition du terrorisme, voy. V.-M. Perez Asinari et Y. Poullet, « The Airline Passenger Data Disclosure Case and the EU-US Debate », *Computer Law and Security Report*, 2002, p. 27. « It should be clear, before any decision be adopted by EU authorities, which is the definition of « terrorism » and any other relevant concept describe in the purposes of US authorities for the processing of personal data with EU origin. This issue seems to be problematic even in the EU side : « [n]either international legal instruments, nor the Framework Decision of the Council on 13th June of 2002 concerning the fight against terrorism have really succeed in overcoming the difficulties traditionally encountered when attempting to give a definition of terrorism which describes its specificity, compared to other forms of organized crime in relation to all its possible forms. However, a sufficiently exact definition of the offence of terrorism is a prerequisite not only for specific indictment, but also for the application of specific procedural rules, particularly in the context of the inquiry of the investigation, and even more so for special forms of detention; otherwise the measures adopt in the fighting terrorism will lack clear legal basis, potentially bringing into question their lawfulness ». EU Network of Independent Experts in Fundamental Rights, The Balance Between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats, Thematic Comment drafted upon request of the European Commission, Unit A5, submitted on 31st March 2003, p. 7. See the analyses on this specific problem made in pages 11-16. See the definitions given in Articles 1 and 2 by the Framework Decision of 13 June 2002 on combating terrorism, OJCE L 164, 22.6.2002, p. 4. See also the Opinion of the Economic and Social Committee on the "ommission Working Document - The relationship between safeguarding internal security and complying with international protection obligations and instruments", 2002/C 149/09, *OJCE* C 149, 21.6.2002, especially points 2.7, 2.9, 2.10 ».

(5) CIS relève à la fois des premiers et troisième piliers. Il s'agit d'une base de données visant à aider les autorités douanières à prévenir, détecter et poursuivre les infractions graves aux lois nationales. Ce système est géré par l'O.L.A.F., l'organisation européenne de lutte antifraude, en coopération étroite avec les directions générales justice et affaires intérieures, d'une part et taxes et douanes, d'autre part. Les données concernent des infractions douanières mais également des données en rapport avec le blanchiment d'argent.

(6) Décision du Conseil 2008/633/JAI du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, *J.O.U.E.* L 218, 13 août 2008. Lire l'avis du contrôleur européen de la protection des données sur la proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière (COM (2005) 600 final), *J.O.U.E.* C 97, 25 avril 2006.

(7) Le nouveau système d'information Schengen « de deuxième génération » (SIS II) remplace SIS I et permet d'élargir l'espace Schengen aux nouveaux États membres de l'U.E. Ce système comporte de nouvelles fonctionnalités. Le 1er juin 2005, la Commission européenne a présenté des propositions en vue de l'établissement du SIS II :

— une proposition de règlement fondé sur le titre IV du Traité CE (visas, asile, immigration et autres politiques liées à la libre circulation des personnes) qui réglementera les aspects du SIS II relevant du premier pilier (immigration) ainsi qu'une proposition de règlement fondé sur le titre V (transports) concernant spécifiquement l'accès des services chargés de l'immatriculation des véhicules aux données du SIS. Ces propositions ont abouti à l'adoption du règlement n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), *J.O.U.E.* L 381, 28 décembre 2006, dite « législation SIS II 1er pilier »

— une proposition de décision fondée sur le titre VI du Traité UE (coopération policière et judiciaire en matière pénale) qui réglementera l'utilisation du SIS à des fins relevant du troisième pilier; cette proposition a quant à elle abouti à l'adoption de la décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération, *J.O.U.E.* L 205, 7 août 2007.

Sur les Accords Schengen I et II, lire S.K. Karanja, *Schengen Information System and Border Control Co-*

cadre d'institutions comme Eurodac[8], Europol[9] et Eurojust[10] contribuent à la création, comme le note le Contrôleur européen de la protection des données (ci après « C.E.P.D. »), d'un « espace européen de liberté, de sécurité et de justice », selon la qualification de l'article 61.1 du Traité de Lisbonne[11]. On ajoute à cela les discussions difficiles[12] de l'article 15 de la directive « protection des données et secteur des communications électroniques » (en abrégé la directive *e-privacy*) qui ont abouti à l'adoption d'une directive sur la conservation des données de communication[13] après de longues hésitations sur la nature juridique de l'instrument propre à la mise en place de cette coopération des opérateurs privés et de l'autorité publique[14].

Au-delà de ces diverses initiatives, le Parlement européen a souhaité dès 2004[15] que soit adopté un « instrument législatif » sur la protection de la vie privée dans le troisième pilier. Le rapport alors remis insistait sur le caractère obligatoire d'un tel instrument qui devait garantir le même niveau de protection que celui atteint dans le premier pilier. On connaît les difficultés d'adoption de ce qui finalement constitue la décision-cadre de protection des données dans le troisième pilier, adoptée le 27 novembre 2008[16], en particulier, les multiples avis du C.E.P.D.[17] et le rapport Roure au Parlement européen[18]. Sans doute est-il bon de rappeler que la solution finalement retenue ne devrait pas couvrir les systèmes déjà mis en place, ainsi notamment les systèmes Eurojust[19] et Europol[20], et ne réglemente, contrairement aux demandes explicites du contrôleur et du Parlement européen, que les seuls flux entre autorités policières et judiciaires nationales et les échanges avec les pays tiers, en laissant aux États membres le soin de réglementer leurs propres activités policières et judiciaires nationales[21].

La décision-cadre, tout comme l'ensemble des textes de l'Union européenne repris ci-dessus et qui encadrent l' « Espace européen de liberté, de sécurité et de justice », trouve le fondement explicite[22] ou implicite de l'atteinte aux libertés, qu'elle légalise, dans l'article 8, § 2, de la Convention européenne des droits de l'homme. L'article 8, § 1er, consacre le droit à la vie privée, mais prévoit des exceptions en son paragraphe 2. La Convention n° 108 du 28 juin 1981, actuellement signée par 43 pays et ratifiée par 39 dont l'ensemble des pays de l'Union européenne traduit les exigences de protection de la vie privée lorsqu'il y a traitement de données à caractère personnel. Elle s'applique à l'ensemble des traitements tant publics que privés et, au sein des premiers, ne distingue en aucune manière les traitements policiers, judiciaires, voire de sûreté nationale. L'affirmation est peu contestable : la recommandation n° R(87) 15 visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police en atteste[23]. Par ailleurs, on connaît la riche et innovante jurisprudence de la Cour de Strasbourg qui progressivement fixe les principes de protection des données applicables aux traitements de données et dont nombre de décisions[24] concernent des traitements policiers, judiciaires ou de sûreté nationale, autant de matières qui relèvent de ce qu'on entend par le troisième pilier, dans le vocabulaire cette fois de l'Union européenne. À l'inverse, la directive européenne 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, directive pourtant héritière de la Convention n° 108[25], a un champ d'application limité au premier pilier et exclut en son article 3, § 2, « en tout état de cause les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État... et les activités de l'État relatives à des domaines du droit pénal. ».

La Convention européenne des droits de l'homme dispose que les autorités judiciaires et policières, voire les services de renseignement et de sécurité publique, justifient toute ingérence dans l'exercice des libertés. À cette fin, il importe que l'ingérence soit « prévue par une loi » (au sens le plus large du terme, sauf lorsque la Constitution d'un pays exige une loi au sens formel du terme) et constitue une mesure qui, dans une société démocratique, est nécessaire soit à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, soit à la défense de l'ordre et la prévention des infractions pénales, soit enfin à la protection d'un intérêt légitime prévalant d'autrui[26]. En outre,

operation : A transparency and Proportionality Evaluation, thèse, Faculté de droit d'Oslo, juin 2006, publié par le Raoul Walhenberg Institute Human Rights Library, M. Nijhoff, Leiden, 2008.

(8) Eurodac est un système d'échange d'informations et de contrôle croisé des empreintes digitales des demandeurs d'asile et des immigrants illégaux suspectés. Eurodac a été mis en place par le règlement n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système « Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace de la Convention de Dublin relative au traitement communautaire des demandes d'asile, *J.O.C.E.* L 316, 15 décembre 2000. Sur le système Eurodac, lire F. Messan, « Le système Eurodac et la protection des données à caractère personnel des demandeurs d'asile », *R.D.T.I.*, 2006, pp. 294 et s.

(9) La création d'Europol a été prévue par le Traité de Maastricht sur l'Union européenne du 7 février 1992. Installé à La Haye, aux Pays-Bas, l'Office a démarré ses activités le 3 janvier 1994. Alors connu sous le nom de « unité "Drogues Europol" » (E.D.U.), il limitait son action à la lutte contre la drogue. Progressivement, d'autres domaines importants de la criminalité lui ont été confiés. Le mandat d'Europol a été étendu le 1er janvier 2002 à toutes les formes graves de la criminalité internationale visées à l'annexe de la convention Europol.

(10) décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, *J.O.U.E.* L 63, 6 mars 2002. Cette unité, qui est dotée de la personnalité juridique, est composée d'un membre national par pays de l'Union, ayant qualité de procureur, de juge ou d'officier de police ayant des prérogatives équivalentes. Compétent pour un large champ d'infractions transnationales, Eurojust poursuit trois objectifs :
— promouvoir et améliorer la coordination des enquêtes et des poursuites entre les autorités compétentes des États membres;
— améliorer la coopération entre ces autorités en facilitant notamment la mise en œuvre de l'entraide judiciaire internationale;
— soutenir les autorités nationales pour renforcer l'efficacité de leurs enquêtes et de leurs poursuites ».

(11) « L'Union constitue un espace de liberté, de sécurité et de Justice dans le respect des droits fondamentaux (...). ». On note la création à Dresde en 2007 du « Future Group », chargé par les ministres des États membres de l'Intérieur et de l'Immigration de préparer l'avenir de cet espace européen et de préparer à leur intention des recommandations de politique stratégique pour l'après 2010. Nous reviendrons (section II) sur le rapport de ce « High Level Advisory Group on the Future of European Home Affairs Policy », préconisant l'équilibre entre les impératifs de mobilité, sécurité et vie privée.

(12) Sur la discussion de cet article 15 et les péripéties qui ont mené à l'adoption de la directive 2006/24/CE, lire les réflexions d'E. Kosta et P. Vaelcke, « Retaining the Data Retention directive », *Computer Law and Security Report*, 2006, pp. 370 et s.

(13) Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données « générées » ou traitées dans le cadre de la fourniture de services de communication accessibles au public ou de réseaux publics de communications et modifiant la directive 2002/58/CE, *J.O.U.E.* L 105, 13 avril 2006.

(14) C.J.C.E., 10 février 2009, *Irlande c. Parlement européen et Conseil*, aff. C-301/06.

(15) Rapport du Comité LIBE (rapporteur Cappato) du 24 février 2004 sur le premier rapport relatif à l'application de la directive protection des données (95/46) (COM(2003)265-C5-0375/2153 (INI).

(16) Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *J.O.U.E.* L 350, 30 décembre 2008.

(17) Premier avis du C.E.P.D. du 19 décembre 2005 sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *J.O.U.E.* C 47, 25 février 2006, deuxième avis du C.E.P.D. du 29 novembre 2006 sur la même proposition, *J.O.U.E.* C 91, 26 avril 2007 et troisième avis du C.E.P.D. du 27 avril 2007, *J.O.U.E.* C 139, 23 juin 2007.

(18) À cet égard, les amendements Roure (du nom du rapporteur au Parlement européen) repris dans le projet de résolution du Parlement européen relative à la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (COM (2005) 475 final) - C 6- 0436/2005 - 2005/0202 (CNS), Doc PE 370.250v02-00).

(19) *Cfr* à ce propos la lettre de M. Kennedy au commissionnaire Vittorino et à Mme Roure rapporteur au Parlement européen de mai 2004, insistant sur le fait que l'application d'un nouveau régime pourrait avoir sur le système bien établi de protection des données existant dans le cadre d'Eurojust et sa crainte d'une diminution du niveau de protection en vigueur. Sur ce point, D. Alonso Blas, « First and Third Pillar : Need for a common approach on Data Protection », in *Reinventing data Protection*, Springer Verlag, Dordrecht, avril 2009.

(20) *Cfr* à ce propos le considérant n° 39 de la décision-cadre : « Plusieurs actes adoptés sur la base du titre VI du Traité sur l'Union européenne comportent des dispositions spécifiques relatives à la protection des données à caractère personnel échangées ou traitées en vertu de ces actes. Dans certains cas, ces dispositions constituent un ensemble complet et cohérent de règles couvrant tous les aspects pertinents de la protection des données. L'ensemble correspondant des dispositions relatives à la protection des données figurant dans ces actes... ne devrait pas être affecté par la présente décision-cadre... ». On note que le texte reste nuancé et n'exclut pas de manière ferme les systèmes Europol, Eurojust auquel se sont ajoutés les systèmes VIS, I et II et les transferts automatisés entre États membres des données A.D.N., données dactyloscopiques et d'immatriculation des véhicules couverts par la décision 2008/615/JAI du Conseil du 23 juin 2008.

(21) Sur ce point, voy. F. Dumortier et Y. Poullet, « La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne », *in Revue Lamy - Droit de l'immatériel*, issue 29, pp. 76-86.

(22) Ainsi, l'article 14.2 de la décision 2002/187/JAI instituant Eurojust du 28 février 2002 qui affirme qu'Eurojust prend les mesures nécessaires pour garantir un niveau de protection au moins équivalent à celui qui résulte de l'application des principes de la Convention n° 108 et de ses amendements subséquents. *Idem* pour l'article 10.1 de la Convention Europol du 26 juillet 1995, *J.O.C.E.* C 317, 27 novembre 1995.

(23) Disponible sur le site du Conseil de l'Europe : http://www.coe.int/T/F/affaires juridiques/. D'autres recommandations du Conseil de l'Europe n'hésitent pas à faire allusion à leur application au secteur policier et judiciaire.

(24) Ainsi, les arrêts *Klass*, *Malone*, *Gaskin*, *Liberty*, *Marper*, etc.

(25) Voy. le considérant n° 11 de la directive : « Considérant que les principes de la protection des droits et des libertés des personnes, notamment le droit à la vie privée, contenus dans cette directive, précisent et amplifie ceux qui sont contenus dans la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des données à l'égard du traitement automatisé des données à caractère personnel ».

(26) Sur la nécessité de distinguer les deux critères à savoir celui formel de l'existence d'une loi prévisible et ac-

cette mesure doit être proportionnée et ne peut être discriminatoire[27].

La jurisprudence de la Cour, la Convention n° 108 et la recommandation R(87) 15 déjà citée, précisent à leur tour ces exigences. On peut estimer comme suit leurs apports[28] :

1) les règles qui entourent la création des traitements de données à caractère personnel dont les finalités ressortissent à la détection d'infractions ou d'activités terroristes doivent être d'autant plus précises et énoncées clairement que les risques d'atteinte à la vie privée et les conséquences dommageables liées à l'utilisation de tels traitements sont élevés[29];

2) la précision doit s'entendre[30] tout à la fois :

— d'une description précise du type d'informations susceptibles d'être enregistrées;

— d'une description précise des catégories de personnes pouvant faire l'objet de mesures de surveillance supposant la collecte et la conservation d'informations;

— d'une description précise des circonstances dans lesquelles de telles mesures peuvent être prises;

— d'une procédure clairement établie de demande d'autorisation pour appliquer ces mesures;

— des limites relatives au stockage d'informations anciennes et à la durée de conservation de nouvelles informations;

— des dispositions détaillées et explicites tant sur les motifs de création des dossiers, la procédure à suivre (pour créer les dossiers ou y accéder), les personnes autorisées à consulter les dossiers, la nature des dossiers, les possibilités d'utilisation des informations contenues dans les dossiers et, le cas échéant, de réutilisation des données pour d'autres finalités[31];

3) il faut éviter, sauf dans des cas de strictes nécessité et proportionnalité, de recourir à la collecte de données relatives à des personnes non soupçonnées d'être impliquées dans des infractions particulières et éviter dans la même mesure le recours à des techniques de profilage et à des dispositifs d'intrusion ou des moyens secrets de collecte d'information[32];

4) il convient, comme le prévoit la recommandation R(87)15, de distinguer à la fois les données factuelles des données résultant d'une évaluation en particulier celles résultant d'opérations automatisées et les différentes catégories de personnes recensées[33] dans les banques de données des services policiers, d'enquête et de sûreté nationale;

5) des limites à la durée de conservation des données doivent être fixées[34]. Par ailleurs, il devrait être interdit de collecter des données pour l'unique motif de l'origine raciale, des convictions religieuses, des comportements sexuels et de l'appartenance à des associations non interdites par la loi;

6) la prise de décision par des ordinateurs vis-à-vis de personnes est contraire à l'exigence de respect de l'identité humaine et ne devrait donc être autorisée que moyennant des garanties strictes;

7) enfin, la jurisprudence du Conseil de l'Europe[35] rappelle à l'envi que de solides garanties doivent être établies par la loi pour permettre un contrôle approprié et efficace des activités de police et des services secrets. Ce contrôle doit exister soit au niveau judiciaire soit au niveau parlementaire et impliquer des autorités indépendantes impartiales et indépendantes afin d'éviter tout abus[36].

Le rappel de ces principes est utile à notre propos. L'objectif des réflexions qui suivent est de démontrer que les textes européens actuels de lutte contre la criminalité ou visant à la création de ce qu'il est convenu d'appeler l'« Espace européen de liberté, de sécurité et de justice »[37] s'éloignent progressivement, mais de manière certaine, de ces principes auxquels l'Union européenne prétend et doit, selon son propre Traité, pourtant se référer. La poursuite de cet objectif suppose, dans un premier temps, la définition de cet « Espace » auquel nous nous référons et l'analyse de la conception européenne des rapports que doivent entretenir droits fondamentaux, d'une part, et impératif de sécurité, de l'autre. Le deuxième temps de notre réflexion rappelle les principes de finalité et de compatibilité pour constater leur affadissement, voire leur non-respect, au fil de l'analyse des textes qui encadrent l'« Espace ». Dans un troisième temps, nous examinons les insuffisances du contrôle juridictionnel européen sur les actes régissant la protection des données en l'état actuel des traités. Enfin, le dernier point se veut plus prospectif : est-il possible — et l'après-Lisbonne y invite — de voir l'Union européenne revenir dans le droit chemin de la protection des données, c'est-à-dire celui que lui indique le Conseil de l'Europe? *Quid* de l'attitude des États nations de l'Union, qui un jour pourraient se trouver coincés devant le choix entre la fidélité vis-à-vis de deux maîtres aux voix contradictoires : l'Union européenne et le Conseil de l'Europe?

2

L'espace de liberté, de sécurité et de justice : vers un « droit à la sécurité »?

Depuis la signature du Traité d'Amsterdam, un des objectifs fondamentaux de l'Union européenne, est d'offrir à ses citoyens un espace de « liberté, de sécurité et de justice » (ci-après « Espace ») sans frontières intérieures. L'« espace normatif » qui découle de cet objectif couvre, d'une part, certaines matières relevant du régime communautaire (premier pilier) — à savoir les politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration, ainsi que la coopération judiciaire en matière civile — et, d'autre part, des matières relevant du régime intergouvernemental (troisième pilier) comme la coopération judiciaire et policière en matière pénale[38].

cessible et celui de fond à savoir l'examen de la nécessité de l'intervention législative dans une société démocratique et la constatation du fait que la Cour se contente bien trop souvent du seul premier critère, lire les réflexions de P. De Hert et S. Gutwirth, « Privacy, data Protection and Law Enforcement, Opacity of the Individual and Transparency of the Power », *in Privacy and the criminal law*, E. Claes, A. Duff and S. Gutwirth (ed.), *Intersentia*, Anvers, 2006, pp. 87 et s.

(27) L'affirmation est martelée par les juges de Strasbourg dans l'affaire *Marper c. Royaume-Uni* jugée le 4 décembre 2008 où il est reproché au Royaume-Uni de prendre des mesures attentatoires à la vie privée des personnes sans se référer à la nature et à la gravité des infractions pour lesquelles les données à leur propos sont collectées

(28) Nous nous inspirons du document publié le 10 décembre 2008 par T. Hammarberg, commissaire aux droits de l'homme auprès du Conseil de l'Europe : « Lutte contre le terrorisme et protection du droit au respect de la vie privée », document disponible sur le site du Conseil de l'Europe, disponible à l'adresse https://wcd.coe.int/ViewDoc.jsp?id=1387723&Site=CM

(29) Dans l'arrêt *Copland c. Royaume-Uni* du 3 avril 2007, la Cour européenne des droits de l'homme a estimé que l'existence dans le droit anglais d'une disposition vague d'habilitation ne suffisait pas et qu'une telle disposition, même si elle était considérée comme satisfaisante par les tribunaux anglais, ne s'apparentait pas à une « loi » au sens de la Convention européenne des droits de l'homme. Mêmes exigences *in* C.E.D.H., aff. *Klass c. Allemagne*, 6 septembre 1978 et *in* aff. *Khan c. Royaume-Uni*, 12 mai 2000. Dans l'affaire C.E.D.H., *AEIH et Ekimdesien c. Bulgarie*, 28 juin 2007, les juges vont plus loin lorsqu'ils notent : « In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated ».

(30) Voy. la recommandation R(87)15, les affaires C.E.D.H., *Kruslin c. France*, 24 avril 1990, *Rotaru c. Roumanie*, 4 mai 2000 et plus récemment aff. *AEIH et Ekimdesien c. Bulgarie*, *op. cit.*

(31) C.E.D.H., aff. *Liberty and others c. Royaume-Uni*, 1er juillet 2008.

(32) C.E.D.H., aff. *Marper c. Royaume-Uni*, *op. cit.*, où le Royaume-Uni est condamné pour maintenir des données DNA de personnes non suspectes.

(33) Dans la même affaire *Marper*, il a également été reproché aux autorités anglaises de ne pas faire suffisamment de distinction dans leurs bases de données DNA entre des personnes coupables et d'autres simplement suspectées.

(34) Le principe est dans la recommandation R(87). Il est rappelé par les juges dans l'affaire *Liberty and others c. Royaume-Uni*, *op. cit.*, et surtout dans l'affaire *Marper* qui condamne le Royaume-Uni pour n'avoir pas fixé de terme à la conservation d'empreintes digitales et donc d'avoir autorisé le maintien de données au-delà de la période pendant laquelle une personne est suspectée.

(35) « La Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus, car un système de surveillance secrète destiné à protéger la sécurité nationale comporte el risque de saper, voire de détruire, la démocratie au motif de la défendre (arrêt *Klass et autres*, pp. 23-24, §§ 49-50... La prééminence du droit implique, entre autres, qu'une ingérence de l'exécutif dans les droits de l'individu soit soumise à un contrôle efficace que doit assumer en dernier ressort, le pouvoir judiciaire, car il offre les meilleurs garanties d'indépendance, d'impartialité et de procédure régulière (arrêt *Klass et autres*, pp. 25-26, § 55) ». C.E.D.H., aff. *Rotaru c. Roumanie*, requête n° 2834/95, 4 mai 2000, p. 17, § 59.

(36) *Cfr* déjà dans C.E.D.H., aff. *Klass c. Allemagne*, *op. cit.* : « The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse... ». Plus récemment dans C.E.D.H., aff. *AEIH et Ekimdesien c. Bulgarie*, *op. cit.* : « In addition in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, the domestic law must provide some protection against arbitrary interference with article 8 rights... The Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment will depend on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering it, the authorities competent to permit, carry out and supervise them and the kind of remedy provided by national law ».

(37) Le Traité de Lisbonne signé en 2007 et actuellement soumis à ratification dans les États membres le rappelle dans son article 2.2 selon lequel l'« Union offre à ses citoyens un espace de liberté, de sécurité et de justice sans frontières intérieures, au sein duquel est assurée la libre circulation des personnes, en liaison avec des mesures appropriées en matière de contrôle des frontières extérieures, d'asile, d'immigration ainsi que de prévention de la criminalité et de lutte contre ce phénomène ».

(38) Rappelons que depuis le Traité de Maastricht, l'Union européenne repose sur trois piliers : les Commu-

Dans ce contexte, cinq ans après avoir adopté un premier programme de travail à Tampere afin d'atteindre ses objectifs, le Conseil en a lancé un second, en 2004 à La Haye, dont la mise en œuvre s'étale jusqu'en 2010. Ce dernier se distingue du premier point. En effet, selon les termes du second programme, « la question de la sécurité de l'Union européenne et de ses États membres se pose avec une acuité renouvelée, au vu notamment des attentats terroristes perpétrés aux États-Unis le 11 septembre 2001 et à Madrid le 11 mars 2004. Les citoyens d'Europe attendent à juste titre de l'Union européenne que, tout en garantissant le respect des libertés et des droits fondamentaux, elle adopte une approche commune plus efficace des problèmes transfrontières tels que l'immigration illégale, la traite des êtres humains, le terrorisme et la criminalité organisée, ainsi que de leur prévention »[39].

Afin de concrétiser ces ambitions « sécuritaires » interpiliers allant de la lutte contre le terrorisme à la prévention et à la répression de l'immigration illégale, le programme de La Haye prône avec insistance une approche innovante de l'échange transfrontière d'informations en matière répressive selon le principe de disponibilité[40], le renforcement du recours à Europol et Eurojust, l'utilisation des données des passagers pour des impératifs de sécurité des frontières et de l'aviation et d'autres fins répressives, l'interopérabilité entre le système d'information Schengen (SIS II), le système d'information sur les visas (VIS) et Eurodac, ainsi que l'intégration « sans tarder, des identificateurs biométriques dans les documents de voyage, les visas, les permis de séjour, les passeports des citoyens de l'U.E. et les systèmes d'information »[41].

Depuis lors, les vœux du Conseil sont loin d'être restés lettre morte. Outre la multiplication des bases de données européennes contenant des éléments biométriques[42], des efforts importants ont été menés en matière d'interopérabilité[43], d'interconnexion[44] — voire de centralisation — de celles-ci, la Commission européenne ayant dévoilé, par exemple, que l'une de ses actions clés pour 2008 consistait en l'établissement d'une « banque » d'empreintes digitales centralisée[45]. Dans un même mouvement, on constate une importante inflation législative dans le domaine de l'échange d'informations[46], appliquant notamment le principe de disponibilité au transfert automatisé des profils A.D.N. et des empreintes digitales[47]. Par ailleurs, force est de constater l'intégration progressive de plus de moyens biométriques d'identification, non seulement dans les visas et les titres de séjour délivrés aux ressortissants de pays tiers[48], mais également dans les passeports et documents de voyage délivrés par les États membres[49]. Enfin, élément non négligeable, ces documents d'identification sont de plus en plus souvent équipés de technologie R.F.I.D.[50] afin de faciliter leur lecture à distance.

Ces nouveaux moyens technologiques mis à disposition des politiques européennes relevant du volet « sécuritaire » de l'Espace traduisent la convergence de plusieurs phénomènes *a priori* hétérogènes les uns aux autres, mais se renforçant mutuellement : la mise en œuvre du nouveau « paradigme sécuritaire », notamment en mêlant les objectifs précédemment indépendants de la lutte contre le terrorisme et la criminalité, d'une part, et de la lutte contre l'immigration illégale[51], d'autre part; la collecte généralisée d'éléments biométriques dans un but d'identification[52] et d'authentification[53] « fiable » des individus; la transmission de ces éléments par radiofréquence (R.F.I.D.)[54] aux

nautés européennes (premier pilier), la politique étrangère et de sécurité commune (deuxième pilier) et la coopération policière et judiciaire en matière pénale (troisième pilier). Ces piliers se distinguent avant tout par le mode de décision employé mais également par la compétence de contrôle de la C.J.C.E. Ainsi, dans le premier pilier, la procédure de décision est de type « communautaire » et implique l'ensemble des institutions. Par contre, dans les deuxième et troisième piliers, elle est de type « intergouvernemental », et le rôle du Parlement est nettement plus effacé. La compétence de la C.J.C.E. est également plus limitée dans le cadre du troisième pilier que dans le cadre du premier. Nous reviendrons sur l'étendue de la compétence juridictionnelle de la Cour au sein du troisième pilier, section III, A).

(39) Programme de La Haye du Conseil, *J.O.U.E.* C 53, 03/03/2005, p. 3, disponible à l'adresse http://ec.europa.eu/justice_home/doc_centre/doc/hague_programme_fr.pdf.

(40) Conformément au programme de La Haye, ce principe signifie que « dans l'ensemble de l'Union, tout agent des services répressifs d'un État membre qui a besoin de certaines informations dans l'exercice de ses fonctions peut les obtenir d'un autre État membre, l'administration répressive de l'autre État membre qui détient ces informations les mettant à sa disposition aux fins indiquées [...] ». Il est par ailleurs souligné dans le programme que « les méthodes utilisées pour échanger les informations devraient exploiter pleinement les nouvelles technologies et être adaptées à chaque type d'information, s'il y a lieu, par le biais d'un accès réciproque aux banques de données nationales, de leur interopérabilité ou de l'accès direct (en ligne) ». Nous revenons sur le principe de disponibilité au titre III, A, de la présente contribution.

(41) Programme de La Haye, *op. cit.*, p. 4

(42) Les bases de données II et VIS contiennent des photographies et des empreintes digitales et Eurodac contient des empreintes digitales. Une nouvelle proposition concerne la collecte d'empreintes digitales dans le cadre d'un système d'entrée/sortie applicable à tous les ressortissants de pays tiers (y compris ceux qui ne sont pas soumis à visa lors de leur première entrée sur le territoire). Voy. la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », COM(2008) 69 final, 13 février 2008. Une autre proposition concerne la création d'un système européen automatisé d'identification criminelle par les empreintes digitales (AFIS) dans lequel seraient rassemblées toutes les données relatives aux empreintes digitales qui ne sont actuellement disponibles que dans les AFIS nationaux. Enfin, une dernière proposition concerne la mise en place d'un « registre européen des documents de voyage et des cartes d'identité » dans lequel les États membres « introduiront aussi les données biométriques enrôlées lors de la demande ». Voy. la communication de la Commission européenne, du 24 novembre 2005, sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, COM(2005) 597 final, non publiée au *Journal officiel*.

(43) Voy. par exemple, la communication de la Commission européenne, du 24 novembre 2005, sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, *op cit.*; et la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », *op cit*.

(44) Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres, *J.O.U.E.* L 93, 7 avril 2009.

(45) Communication de la Commission au Conseil et au Parlement européen, au Comité économique et social et au Comité des Régions du 21 février 2007, Stratégie politique annuelle pour 2008, COM(2007)65

(46) Voy. par exemple, la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité; le Traité de Prüm, signé par sept États membres (Allemagne, Autriche, Belgique, Espagne, France, Luxembourg et Pays-Bas), *J.O.* C 71/35 du 28 mars 2007; les décisions 2008/615/JAI, 2008/616/JAI et 2008/617/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (intégrant le Traité de Prüm dans l'ordre juridique de l'U.E.). Voy. également la proposition de décision-cadre du Conseil relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les États membres, COM(2005) 690 final.

(47) Voy. par exemple les articles 2 à 9 de la décision 2008/615/JAI, *op. cit.*

(48) Règlement (CE) nº 1030/2002 du Conseil, du 13 juin 2002, établissant un modèle uniforme de permis de séjour pour les ressortissants de pays tiers; proposition de règlement du Conseil modifiant le règlement (CE) nº 1030/2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, COM(2003) 0558, non publié au *Journal officiel*.

(49) Règlement (CE) nº 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres; décision de la Commission du 28 juin 2006 établissant les spécifications techniques afférentes aux normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, C(2006) 2909 final, non publié au *Journal officiel*. Depuis août 2006, les États membres délivrent des passeports biométriques contenant l'image faciale numérisée du titulaire; à partir du 28 juin 2009, les passeports contiendront également les empreintes digitales.

(50) En vertu de la décision de la Commission du 28 juin 2006, précitée, les États membres sont tenus d'utiliser des puces R.F. (à radiofréquences) comme support de stockage dans leurs documents de voyage et leurs passeports.

(51) À cet égard, le Conseil « justice et affaires intérieures » qui s'est réuni à Luxembourg les 12 et 13 juin 2007 illustre bien cette confusion des objectifs entre criminalité, terrorisme et immigration. À cette occasion, le Conseil a en effet a invité la Commission à présenter dans les plus brefs délais une modification du règlement Eurodac afin de permettre aux services de police et aux services répressifs des États membres ainsi qu'à Europol d'avoir accès, dans certaines conditions, à Eurodac, base de données conçue initialement comme instrument pour l'application du règlement de Dublin.

(52) L'identification permet de connaître une identité d'une entité, c'est-à-dire de déterminer l'identité d'un individu au sein d'une certaine population, elle nécessite une « one-to-many comparison » afin d'identifier l'utilisateur parmi l'ensemble des personnes enregistrées. Voy. la définition proposée à l'ISO : « Recognizing an entity within some context with unique identity references and additional information that characterizes the entity » (http://www.jtc1sc27.din.de/sce/SD6).

(53) L'authentification est un processus qui consiste à vérifier l'identité prétendue d'une personne donnée afin d'obtenir l'assurance que l'individu est bien la personne qu'il prétend être, elle ne nécessite qu'une « one-to-one comparison », une comparaison des données transmise avec l'information préalablement enrôlée appartenant à une seule personne. Voy. la définition de l'ISO : « Provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication) » (ISO/IEC 18028-4 : 2005).

(54) Dans son projet de recommandation sur la mise en œuvre des principes relatifs à la vie privée, la protection des données et la sécurité de l'information dans les applications soutenues par la R.F.I.D. de février 2008, la Commission définit l'identification par radiofréquence (R.F.I.D.) comme « l'utilisation d'ondes électromagnétiques ou d'un couplage de champ réactif dans la portion de fréquence radio du spectre pour communiquer en direction ou en provenance d'une étiquette à travers différents schémas de modulation et d'encodage, et cela en vue de lire de façon exclusive l'identité d'une étiquette radiofréquence ou d'autres données stockées sur elle ».. La Commission a également rappelé son intérêt pour la technologie R.F.I.D. dans sa communication au Parle-

autorités jugées compétentes; l'interopérabilité des bases de données en vue de leur interconnexion; et enfin, un échange accru d'informations, échange rendu possible grâce au principe de disponibilité. L'ensemble de ces caractéristiques préfigure un espace de justice, de liberté et de sécurité basé sur une large dissémination de « capteurs » (R.F.I.D. et biométriques) couplés à de larges bases de données interconnectées permettant le contrôle à distance des individus grâce à des processus ubiquitaires, opaques et automatiques[55] de croisement de données présumées exactes.

Ce premier volet sécuritaire paraîtrait quelque peu orwelien s'il n'était accompagné de mesures destinées à garantir les droits fondamentaux des personnes concernées, en particulier leur droit au respect de la vie privée. À ce sujet, l'on a déjà rappelé que l'article 61.1 du Traité de Lisbonne, déjà cité, dispose que « l'Union constitue un espace de liberté, de sécurité et de justice dans le respect des droits fondamentaux [...] ». Loin d'être une profession de foi purement formelle, cette exigence semble avoir largement été prise à cœur par les institutions. Outre les nombreuses dispositions relatives à la protection des données à caractère personnel dont regorgent les textes législatifs susmentionnés[56], la matière fait l'objet d'un maillage législatif fort complexe en droit européen. Les directives 95/46/CE[57] et 2002/58/CE[58] s'appliquent aux domaines relevant du pilier communautaire, une décision-cadre couvre les matières relevant du troisième pilier[59], la convention d'application de l'Accord de Schengen[60] contient des dispositions spécifiques sur la protection des données applicables au système d'information Schengen, la Convention Europol[61] contient entre autres, les règles relatives à la transmission de données à caractère personnel par Europol à des États et des instances tiers et la décision créant Eurojust[62] renvoie aux dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel.

Tant le volet sécuritaire que celui relatif à la protection des données font donc l'objet d'une attention toute particulière de la part des institutions chargées de concrétiser l'espace de liberté, de sécurité et de justice. Depuis le Traité d'Amsterdam, « droits fondamentaux » et « sécurité » sont ainsi devenus les deux poids principaux de la « balance » qu'ont pour mission d'équilibrer les institutions européennes dans le respect des valeurs démocratiques chères à l'Europe.

Dans cet esprit, un groupe de travail (ci-après « Future Group » [63]) a été mis sur pied en 2007 par les ministres de l'Intérieur et de l'Immigration en vue de conseiller les institutions pour préparer le programme de travail post-La Haye. Afin de résoudre l'épineuse question des liens et rapports que doivent entretenir entre eux les concepts de « droits fondamentaux » et de « sécurité », le « Future Group » recourt précisément à cette métaphore de la « balance ». Dans son rapport, le groupe propose ainsi de « préserver le modèle européen dans le domaine des affaires intérieures en mettant en balance mobilité, sécurité et vie privée »[64].

Certes, ce groupe n'est pas l'inventeur du concept de la « balance » dans le domaine qui nous intéresse, la notion faisant malheureusement partie du langage politique de l'Union depuis quelques années.[65] Nous restons cependant abasourdis de voir figurer, dans un document d'orientation officiel ayant pour vocation d'inspirer le futur programme de Stockholm, la référence à la « balance » — un instrument de mesure du poids — comme outil permettant de résoudre la délicate équation impliquant « droits fondamentaux » et ce que certains qualifient à tort de « droit à la sécurité ».

Il convient en effet de rappeler avec force, qu'à l'inverse du droit au respect de la vie privée, — protégé notamment par l'article 8 de la Convention européenne des droits de l'homme — le droit fondamental à la sécurité, parfois invoqué comme contrepoids au premier droit, ne fait l'objet d'aucune consécration juridique. Explicitons ce dernier propos. Il est vrai, certes, qu'outre le droit au respect de la vie privée, l'organisation politique a également le devoir d'assurer à chacun le droit « à la sûreté de sa personne »[66]. Cependant, il importe de signaler que ce droit à la sûreté signifie tout autre chose qu'un droit à la sécurité. Il implique, entre autres, un devoir pour l'organisation politique d'assurer à chaque être humain de ne pas être arrêté ni détenu arbitrairement. À cet égard, il est intéressant de relever que, paradoxalement, l'effectivité de ce dernier droit est rendue moins certaine à la suite de l'utilisation de certaines technologies, particulièrement lors de périodes troubles. Ainsi, Marc Rotenberg a vivement critiqué la récente initiative militaire des États-Unis visant à utiliser des scanneurs mobiles afin de collecter les empreintes digitales et les iris de centaines de milliers d'Irakiens dans le but de les profiler. Selon cet auteur, « the new system of biometric identification and secret profiles raises the very real possibility of future reprisals and killings on a far more widespread basis »[67].

Quant à la « sécurité », celle-ci n'a jamais été conçue comme un « droit » ayant un « poids » équivalent à ceux consacrant, par exemple, la dignité et le respect de la vie privée. Deux raisons suffisent à justifier cette conception. Non seulement un « droit à la sécurité » serait susceptible de multiples interprétations contradictoires[68], mais plus fondamentalement, dans la logique des déclarations fondamentales, c'est par le respect de l'ensemble des droits civils, politiques et socio-économiques que ces déclarations proclament qu'un État de droit vise à assurer à l'homme la sécurité civile, politique et socio-économique qui lui revient. La sécurité et la paix par la liberté, tel est le credo des droits de l'homme[69].

ment européen, au Conseil, au Comité économique et social et au Comité des régions sur « L'identification par radiofréquence (R.F.I.D.) en Europe : vers un cadre politique », COM(2007) 96 final.

(55) La Commission prévoit de mettre en place un système d'entrée/sortie dans l'U.E. au moyen de « barrières automatiques ». Les voyageurs de bonne foi et les ressortissants de l'U.E. qui possèdent un passeport électronique pourraient faire l'objet d'une vérification automatisée à leur arrivée via un dispositif qui effectuerait une comparaison entre les identifiants biométriques du voyageur d'une part, et les données biométriques intégrées dans les documents de voyage ou dans une base de données d'autre part. Voy. la communication de la Commission, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », *op. cit.*

(56) Voy. par exemple les articles 6, 7 et 17 de la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, précitée; les articles 8 et 9 de la décision-cadre 2006/960/JAI, précitée; les articles 24 à 32 de la décision-cadre 2006/960/JAI, précitée; l'article 4 du règlement (CE) nº 1030/2002, précité et l'article 4 du règlement (CE) nº 2252/2004, précité.

(57) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.* L 281 du 23 novembre 1995, pp. 31-50.

(58) Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.* L 201 du 31 juillet 2002, pp. 37-47.

(59) Pour avoir un aperçu des difficultés relatives à la détermination des champs d'application respectifs de la directive 95/46/CE et la proposition de décision-cadre, voy. F. Dumortier et Y. Poullet, « La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne », *in Revue Lamy - Droit de l'immatériel*, nº 29, pp. 76-86.

(60) Convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la république fédérale d'Allemagne et de la république française relatif à la suppression graduelle des contrôles aux frontières communes, *J.O.* C 239 du 22 septembre 2000, p. 19.

(61) Articles 104 à 118 de la Convention sur la base de l'article K.3 du Traité sur l'Union européenne portant création d'un Office européen de police (Convention Europol), *J.O.* C 316 du 27.11.1995, p. 2.

(62) Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, *J.O.* L 63 du 6 mars 2002, p. 1.

(63) Le « Future Group » est un groupe de travail informel mis en place en 2007, à Dresde, par les ministres de l'intérieur et de l'Immigration en vue de préparer l'avenir de l'espace européen de justice, de liberté et de sécurité. La raison d'être du groupe fut de rédiger un rapport politique contenant des recommandations qui serviront de « source d'idées » à la Commission européenne et aux États membres dans la conception des politiques dans le domaine des affaires intérieures après 2010.

(64) Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy, précité, p. 17. Selon le groupe, « one priority for each proposal based on the post-Hague Programme (...) will be the reflection on how to balance mobility, security and privacy in a proportionate way. There is a need to overcome the stereotype of seeing security, mobility and privacy as opposing concepts which exclude each other. Therefore, under the post-Hague Programme, an intensive public debate including a substantial inter-institutional discussion involving the European and national parliaments will have to be launched on how to address the current equilibrium in a way that allows for significantly improved security, at the same time as equally enhanced privacy and mobility ». Son rapport contient d'ailleurs non moins de seize occurrences de cette notion.

(65) En 2004, M. Frattini, commissaire chargé de l'Espace J.L.S. déclarait que « new balances must be found between privacy and security » (SPEECH/04/549 disponible à l'adresse http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/04/549&format=HTML&aged=1&language=EN&guiLanguage=en). Le 7 septembre 2005, la présidence britannique de l'Union européenne rédigeait déjà un document de travail intitulé « Liberty and security, striking the right balance ». Utilisant à nouveau la métaphore de la balance, la Commission européenne lança un programme intitulé « Security and safeguarding Liberties » au sein des perspectives financières 2007-2013 (disponible à l'adresse http://ec.europa.eu/justice_home/funding/intro/funding_security_en.htm).

(66) Voy. article 3 de la D.U.D.H.

(67) Voy. EPIC, http://epic.org/privacy/biometrics/epic_iraq_dtbs.pdf; s'il est vrai que la situation politique actuelle en Irak diverge fortement du contexte européen, il n'en a toutefois pas toujours été ainsi. Rappelons, en effet, que sous l'occupation française durant la Seconde Guerre mondiale, tout comme en Irak actuellement, de nombreuses personnes avaient eu la vie sauve en utilisant de fausses identités. Or, l'utilisation généralisée d'identifiants biométriques et de technologie R.F.I.D. dans les documents de voyage couplée à des bases de données interconnectées rend bien plus difficile la dissimulation de l'identité et peut donc faciliter les contrôles discriminatoires ainsi que la détention arbitraire.

(68) Parle-t-on de sécurité sociale, politique, économique, culturelle, psychique, juridique ou physique?

(69) Voy. notamment le préambule de la Convention euorpéenne des droits de l'homme selon lequel « les li-

C'est cette logique que renverse Antonio Vitorino, ancien commissaire européen chargé de la justice et des affaires intérieures, lorsqu'il déclare que « la sécurité ne se limite pas à la répression de la criminalité : c'est un moyen pour atteindre la liberté »[70]. En d'autres termes, certains responsables politiques n'hésitent pas à affirmer que le droit à la sécurité est une condition de la reconnaissance des autres droits fondamentaux. Bref, il est d'une importance cruciale pour la démocratie que la métaphore de la « balance » ne conduise pas à confondre la fin et les moyens : c'est par l'assurance étatique de la jouissance effective de ses droits fondamentaux que l'homme peut espérer vivre en paix et en sécurité, et non le contraire.

En adhérant prochainement à la Convention européenne des droits de l'homme, c'est à cet engagement qu'ont choisi de souscrire les institutions européennes. Tant dans la conception que dans la mise en œuvre de leurs politiques, elles ont pour obligation de respecter les droits de l'homme en tant que limite et fondement du pouvoir afin que la finalité de celui-ci reste au service de l'homme et de ses droits. C'est pourquoi elles doivent s'atteler à atteindre leur objectif de sécurité par le respect effectif des droits de l'homme, au risque de confirmer la thèse bien connue d'Agamben et de Carl Schmitt selon laquelle l'« état d'exception » deviendrait la véritable source du droit[71].

Cette dernière remarque est particulièrement importante dans le contexte européen actuel où la sécurité de l'Espace est censée reposer sur des mécanismes performants d'échanges d'informations entre les autorités nationales et les acteurs européens. Dans un tel environnement (ou devrait-on dire « réseau ») de données, le respect des droits de l'homme passe essentiellement par le respect des principes fondamentaux de protection des données à caractère personnel. Les textes actuels de l'Union européenne consacrent-ils pas le respect des principes de finalité et de compatibilité qui sont au cœur de la protection des données? Notre réponse est pour le moins dubitative.

3

Quelle liberté dans l'Espace de sécurité? Vers une érosion du principe de finalité dans le droit de l'Union

Le principe clef européen de la protection des données à caractère personnel est le principe de finalité déterminée[72]. Il exige, d'une part, que les données ne soient collectées que pour une finalité déterminée, explicite et légitime, et, par là, interdit la collecte de données pour des finalités inconnues. D'autre part, il exige que des données collectées initialement pour une finalité déterminée ne puissent être traitées ou divulguées ultérieurement que si le traitement ultérieur, outre le fait qu'il ait également une finalité déterminée, est compatible avec la finalité initiale. Ces deux principes reflètent l'idée qu'un traitement de données à caractère personnel doit offrir un certain degré de prévisibilité et de transparence à l'égard des personnes concernées. Le traitement ultérieur compatible n'est pas défini *in extenso*. Sont considérés comme compatibles, les traitements qui entrent dans les prévisions raisonnables de la personne concernée[73] ou encore, les traitements ultérieurs déterminés par la loi.

Or, on observe que dans le cadre de la réalisation de l'Espace le droit de l'Union multiplie les glissements de finalités. En effet, à la suite des attaques terroristes du 11 septembre, l'Union européenne a adopté plusieurs instruments qui rendent compatible le traitement ultérieur par la police à des fins de lutte contre le terrorisme et la criminalité grave, des données collectées initialement par des services de police dans le cadre d'enquêtes pénales, affirmant ainsi le principe de disponibilité (A). L'Union étend également cette disponibilité à et vis-à-vis d'autres autorités à des fins de visa, d'immigration, de douanes selon le principe d'interopérabilité (B), voire vis-à-vis d'entreprise privées telles les sociétés d'aviation, de télécoms et financières selon le principe de coopération du secteur privé (C)[74].

Enfin, nous analyserons la décision-cadre relative à la protection des données dans le cadre de la coopération policière et judiciaire, dont la faiblesse des dispositions confirme l'érosion du principe de finalité dans l'Espace (D), avant d'évoquer les discussions actuelles au sein de l'Union européenne visant à établir une stratégie globale d'échange d'informations policières à des fins de lutte contre le terrorisme et la criminalité grave (E).

A. — Le principe de disponibilité et la compatibilité du traitement ultérieur de données de police par les services de police d'autres États membres

Le principe de disponibilité est défini dans le programme de La Haye, comme la possibilité pour « Tout agent des services répressifs d'un État membre qui a besoin de certaines informations dans l'exercice de ses fonctions de les obtenir d'un autre État membre, les services répressifs de l'autre État membre qui détient ces informations les mettant à sa disposition aux fins indiquées »[75]. Il est le principe autour duquel s'articule le renforcement de l'échange d'informations entre États membres dans le cadre de la coopération policière et judiciaire. Il faut toutefois rappeler que le principe de disponibilité a été posé une première fois en dehors du champ de l'Union européenne. Le Traité de Prüm, conclu par sept États membres consistait en une sorte de « vraie-fausse coopération renforcée »[76] sur « l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontière et la migration illégale »[77]. L'accord visait entre autres la mise en place de fichiers A.D.N. et l'échange d'informations résultant de ces fichiers, mais aussi l'échange d'empreintes digitales et la possibilité de consultation automatisée des registres d'immatriculation de véhicules. Nous verrons que l'essentiel des dispositions de ce Traité aura inspiré l'adoption d'une décision au niveau européen, dite décision *Prüm*, consistant à intégrer en substance les dispositions de ce Traité dans l'Union européenne. Le principe de disponibilité emporte, en pratique, plusieurs déclinaisons qu'il est utile de distinguer. D'une disponibilité à la demande, l'Union européenne avance peu à peu vers le principe d'une disponibilité en ligne des données. Enfin, le principe de disponibilité est parfois amené à jouer envers les États tiers.

Le principe de disponibilité à la demande consiste en la possibilité pour les services répressifs d'un État membre d'avoir accès, sur demande, aux données détenues par un autre État Membre dans le but d'effectuer un traitement ultérieur à des fins policières. L'article 3 de la décision-cadre suédoise[78] dispose en son point 1 que : « les États membres veillent à ce que les informations — tout type d'information détenues par un service répressif ou par des autorités publiques ou des entités privées et accessibles aux services répressifs — puissent être transmises aux services répressifs compétents des autres État membre. (...) ». Il précise au point 2 que : « les informations sont transmises à la demande d'un service répressif compétent (...) ». Le principe de disponibilité à la demande, tel que défini dans la décision-cadre vise alors à rendre l'échange d'informations rapide et efficace dans le cadre d'enquêtes pénales ou d'opérations de renseignement en matière pénale[79]. La décision *Prüm* adoptée en 2008

bertés fondamentales constituent les assises mêmes de la justice et de la paix dans le monde ».

(70) Voy. http://ec.europa.eu/archives/commission_1999_2004/vitorino/index_en.htm.

(71) Voy. G. Agamben, *État d'exception - Homo sacer*, Seuil, 2003 et C. Schmitt, *Théologie politique*, 1922, rééd. Gallimard, 1988. Selon Schmitt, « Est souverain celui qui décide de la situation exceptionnelle » et « il est impossible d'établir avec une clarté intégrale les moments où l'on se trouve devant un cas de nécessité (Notfall) ni de prédire, dans son contenu, ce à quoi il faut s'attendre dans ce cas ».

(72) Il est énoncé à l'article 5, *b*, de la Convention 108 et à l'article 6, § 1er, *b*, de la directive 95/46.

(73) Voy. notamment article 4, § 1er, de la loi belge de protection de la vie privée du 8 décembre 1992, *M.B.*, 18 mars 1993

(74) Dans le même sens voy. S. de Biolley, « Collecte, échange et protection des données dans la coopération en matière pénale », *J.T.D.E.*, septembre 2006, pp. 196-199, en particulier ses développements sur « le principe de disponibilité », « l'interopérabilité des bases de données de sécurité intérieure » et « l'utilisation des données produites par le secteur privé ».

(75) Voy. point 2.1 du programme de La Haye du Conseil, *J.O.U.E.* C 53, 3 mars 2005, et considérant 4 de la décision 2008/615/JAI, du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière dite décision *Prüm*, *J.O.U.E.* L 210, 6 août 2008.

(76) Lire J. Ziller, « Le Traité de Prüm, une vraie-fausse coopération renforcée dans l'Espace de sécurité de liberté et de justice », European University Institute, Working Paper nº 2006/32. L'auteur rappelle à juste titre que le Traité de Prüm rentre dans la thématique du troisième pilier. Pourtant les États signataires, seulement au nombre de sept ont choisi d'agir en dehors des traités européens, tandis que le mécanisme de coopération renforcée prévoit la participation d'au minimum huit États.

(77) Traité entre le royaume de Belgique, la république fédérale d'Allemagne, le royaume d'Espagne, la république française, le grand-duché de Luxembourg, le royaume des Pays-Bas et la république d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, signé à Prüm (Allemagne), le 27 mai 2005.

(78) Décision-cadre 2006/960/JAI du 18 décembre 2006 relative à la simplification de l'échange d'information et de renseignement entre les services répressifs des États membres de l'Union européenne, *J.O.U.E.* L 386, 29 décembre 2006.

(79) Article 1er, § 1er, de la décision-cadre 2006/960/JAI, du 18 décembre 2006.

élargit les finalités pour lesquelles un échange de données à caractère personnel sur demande ou d'initiative doit s'opérer, puisqu'elle vise désormais la prévention de ces infractions pénales[80]. Elle prévoit qu'aux fins de prévention des infractions pénales et du maintien de l'ordre et de la sécurité publique lors de manifestations de grandes envergures ainsi qu'aux fins de prévention des infractions terroristes, les États membres sont tenus de transmettre les données demandées par un autre État membre[81]. D'abord applicable aux fins d'enquête pénale pour des infractions déjà commises, le principe de disponibilité sur demande vient désormais s'appliquer aux finalités de prévention de ces infractions.

Outre la disponibilité à la demande, l'Union européenne entend favoriser une déclinaison renforcée du principe, en développant le principe de disponibilité en ligne des données. L'idée de mettre en place une disponibilité en ligne de certaines données est directement inspirée du Traité de Prüm qui prévoyait déjà un tel dispositif. La décision *Prüm*[82] intègre ce principe en prévoyant qu'aux fins d'enquête en matière d'infractions pénales, l'accès aux données A.D.N. et aux empreintes digitales détenues par les États membres pourra avoir lieu via la possibilité d'une consultation automatisée de ces données[83]. Enfin, le principe de disponibilité en ligne qui ne touche jusqu'ici que certaines données devrait trouver une application généralisée. C'est l'objet de la proposition de décision-cadre du Conseil relative à l'échange d'information en vertu du principe de disponibilité du 12 octobre 2005[84] qui pose le principe d'un accès en ligne aux informations disponibles et aux données d'index non disponibles en ligne[85]. Il sera alors possible de savoir si les informations recherchées sont disponibles avant même d'émettre une demande d'information. Les informations seront accessibles aux autorités compétentes des États membres, ainsi qu'à Europol, et ceci aux fins de prévention ou de détection des infractions pénales ou aux fins d'enquêtes en la matière. En plus de s'appliquer à un éventail très large de finalités (prévention, détection des infractions pénales), le respect du principe de finalité risque de devenir illusoire. Compte tenu des différences parfois importantes qui existent dans la portée des compétences des autorités des États membres, le risque que certaines données recueillies pour une finalité précise soient ensuite traitées pour une autre finalité est un enjeu dont la décision-cadre ne pourra pas faire l'économie[86].

Enfin, l'échange d'informations sous le principe de disponibilité emporte aussi certaines implications en dehors de l'Union. Le programme américain d'exemption de visa (Visa Waiver Program) permet aux citoyens de certains pays d'entrer aux États-Unis pour un voyage de tourisme ou d'affaires sans avoir à obtenir au préalable un visa de non-immigrant. En échange, les États-Unis négocient avec les États membres de l'Union européenne des accords bilatéraux (Mémorandum of Understanding (MoU)) relatifs à l'accès aux banques de données des États européens en faveur des États-Unis.

B. — Le principe d'interopérabilité : compatibilité du traitement ultérieur à des fins policières des données de douane, d'immigration et de visa ?

Le concept d'interopérabilité est défini dans la communication de la Commission sur l'interopérabilité des bases de données européennes[87] comme « la capacité qu'ont les systèmes d'information et les processus opérationnels dont ils constituent le support d'échanger les données et d'assurer le partage des connaissances ». Selon une vision très restrictive de la Commission, l'interopérabilité serait un concept technique plutôt que juridique ou politique. Le contrôleur européen de protection des données (C.E.P.D.) ne partage pas entièrement ce point de vue[88]. En effet, le C.E.P.D. considère que lorsque l'on parle d'interopérabilité, « il ne s'agit pas seulement de l'utilisation en commun de systèmes d'information à grande échelle, mais également de possibilités d'accès aux données, d'échange de données ou même de fusion de bases de données ». Le C.E.P.D. ajoute : « cette communication de données entend proposer, pour les systèmes d'information à grande échelle, de nouveaux objectifs allant au-delà de la finalité initiale de ces systèmes, ce qui rend automatiquement nécessaire une nouvelle analyse complète de l'impact de cet objectif sur la protection des données personnelles ». La définition proposée par la Commission est étroite en ce qu'elle réduit le concept d'interopérabilité à l'interconnexion de systèmes, en évacuant volontairement les dimensions politique et légale, mais aussi économique, sociale, culturelle ou sémantique de ce concept[89]. Nous envisageons trois types d'interopérabilité : (1) l'interopérabilité entre les bases de données de VIS, (2) l'interopérabilité entre les bases de données d'immigration et, enfin, (3) l'interopérabilité entre les bases de données des douanes.

1. — Tel que le C.E.P.D. l'a fortement souligné, le Visa Information System (VIS)[90] est initialement un système d'information « mis au point aux fins de l'application de la politique européenne en matière de visas et non comme instrument de répression »[91]. L'adoption d'une décision du Conseil concernant l'accès en consultation au système VIS prévoit désormais que « les autorités désignées des États membres et l'Office européen de police (Europol) peuvent avoir accès en consultation au système d'information sur les visas (VIS), aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière »[92]. Cette décision s'inscrit dans la lignée de la Communication de la Commission en proposant une première application du principe d'interopérabilité[93]. Initialement collectées à des fins de politique de visas, ces données sont désormais accessibles à des fins de lutte contre le terrorisme.

2. — Eurodac[94], banque de données centralisée contenant notamment les empreintes digitales des demandeurs d'asile et des immigrants clandestins, intéresse les services répressifs des États membres[95]. C'est ce qui ressort des conclusions[96] du Conseil du 12 et 13 juin 2007, où ce dernier « estime qu'afin de remplir pleinement l'objectif d'amélioration de la sécurité et de renforcer la lutte contre le terrorisme, il convient d'accorder aux services de police et aux services répressifs des États membres, ainsi qu'à Europol, l'accès au système Eurodac, à certaines conditions et à des fins de consultation, dans le cadre de l'exercice de leur compétences dans le domaine de la prévention et de la détection des infractions terroristes et autres infractions pénales graves et des enquêtes en la matière »[97]. Ainsi, une proposition de décision[98] du Conseil a vu le jour. Elle vise à

(80) Article 1er de la décision *Prüm*, 2008/615/JAI, du 23 juin 2008 : « Par la présente décision, les États membres visent à approfondir la coopération transfrontalière...en particulier l'échange d'informations entre les services chargés de la prévention des infractions pénales et des enquêtes en la matière ».

(81) Article 13, 14 et 16 de la décision *Prüm*, 2008/615/JAI, du 23 juin 2008.

(82) Article 3, § 1er, 4, 2, § 1er et 8, de la décision *Prüm*, 2008/615/JAI, du 23 juin 2008.

(83) Voy. le chapitre 2 de la décision *Prüm*, 2008/615/JAI, du 23 juin 2008.

(84) Proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité du 12 octobre 2005, COM(2005)490 final.

(85) Article 9 de la proposition de décision-cadre relative à l'échange d'informations en vertu du principe de disponibilité.

(86) C'est ce que le C.E.P.D. rappelle dans son avis sur à la proposition de décision-cadre relative à l'échange d'informations en vertu du principe de disponibilité du 28 février 2006, *J.O.U.E.* C 116, 17 mai 2006.

(87) Communication de la Commission au Conseil et au Parlement européen sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergie entre ces bases, 24 novembre 2005, COM(2005) 597 final, non publié au *J.O.*

(88) Observations du C.E.P.D. relatives à la communication de la Commission sur l'interopérabilité des bases de données européennes, Bruxelles, le 10 mars 2006.

(89) P. De Hert et S. Gutwirth, « Interoperability of police databases within the EU : an accountable political choice? », TILT Law & Technology Working Paper Series, no 001/2006, avril 2006, disponible sur http://ssrn.com/abstract=971855.

(90) Décision 2008/633/JAI du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins d'enquête en la matière, *J.O.U.E.* L 218, 13 août 2008.

(91) Avis du contrôleur européen de la protection des données sur la proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière (COM (2005) 600 final), *J.O.U.E.* C 97, 25 avril 2006.

(92) Article 1er de la décision 2008/633/JAI du 23 juin 2008.

(93) Lire l'avis précité du C.E.P.D. où il situe l'importance de la proposition dans la tendance actuelle à renforcer l'interopérabilité des bases de données telle que préconisée par la Commission.

(94) Règlement no 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système « Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace de la Convention de Dublin.

(95) L'accès à Eurodac par les services répressifs a été fortement défendu par le ministre de l'Intérieur d'Autriche, Kurt Hager, à l'occasion de la conférence organisée par la Commission européenne, les 19 et 20 mai derniers à Bruxelles sur le thème « Data Protection, more use, more protection? ».

(96) Conclusions du Conseil de l'Union européenne concernant l'accès des services de police et des services répressifs des États membres, ainsi que d'Europol, au système Eurodac; 2807e session du Conseil justice et affaires intérieures, Luxembourg, les 12 et 13 juin 2007.

(97) Pour un aperçu général de la compétence, des instruments et des mesures développées par l'U.E. dans le cadre de la lutte contre le terrorisme et la criminalité d'une part, et la politique d'asile et d'immigration d'autre part et les relations de ces politiques entre elles, voy. notamment J. Lodge, « Sustaining freedom, security and justice - From terrorism to immigration », *Liverpool Law Review*, 2002, pp. 41-71.

(98) Proposition de décision du Conseil relative aux demandes de comparaison avec les données EURODAC

accorder aux services de police et aux services répressifs des État membre, ainsi qu'à Europol, l'accès au système Eurodac.

3. — Le système d'informations douanier (S.I.D.)[99] intéresse également Europol et Eurojust. L'objectif de la Convention sur l'emploi de l'informatique dans le domaine des douanes vise à aider « à prévenir, rechercher et poursuivre les infractions graves aux lois nationales ». Invoquant les limites de la Convention pour atteindre pleinement cet objectif et la nécessité d'assurer une plus grande complémentarité avec l'action menée au niveau d'Europol et Eurojust, une initiative française de décision propose de permettre à ces agences d'accéder, dans les limites de leur mandat respectif, aux données introduites dans le système d'information douanier[100].

Les risques qu'entraîne l'interopérabilité des systèmes sur le principe de finalité ont été parfaitement exprimés par Paul De Hert et Serge Gutwirth : « Interoperability, made possible by law, disrespects the importance of separated domains and cuts through their protective walls (...). In other words, one policy aim, one good, for instance security, is taken as an absolute. Questions about the necessity of trust based on the plurality of societal goods, translated into data protection as the purpose specification principle, are left unanswered »[101]. L'interopérabilité des bases de données européennes a pour effet d'éroder considérablement le principe général de finalité déterminée, mais plus généralement les valeurs portées par la protection des données à caractère personnel, c'est-à-dire limiter la concentration excessive de données par les autorités publiques et garantir aux individus un degré élevé de transparence.

C. — **Le principe de coopération : compatibilité du traitement ultérieur à des fins policières de données commerciales détenues par des opérateurs privés?**

L'érosion du principe de finalité se traduit également dans le recours croissant des autorités policières aux données collectées initialement par le secteur privé pour leurs finalités commerciales propres, notamment certaines données télécom, financières et relatives aux passagers des transports aériens.

1. — En ce qui concerne les données télécom, la directive 2006/24 relative à la conservation des données constitue un premier exemple de traitement ultérieur à des fins répressives des données commerciales. Elle prévoit la conservation, pendant une durée de six à vingt-quatre mois, des données de trafic, d'identification et de localisation afin d'en permettre l'accès à des services de police à des fins de recherche, de détection et de poursuite d'infractions graves. Les données sont ici conservées en vue d'enquêtes potentielles futures. La finalité avancée d'un tel dispositif de conservation pose un certain nombre de questions. Le renvoi au droit national pour la définition des « infractions graves » pour lesquelles l'accès aux données des services de police et judiciaires est permis laisse aux États membres une marge d'appréciation extrêmement large.

2. — En ce qui concerne les données financières, il faut se référer à l'affaire Swift, société de droit belge, qui gère les échanges internationaux de quelque huit mille institutions financières situées dans 208 pays. En 2006, le *New York Times* révèle que Swift a, depuis les attentats du 11 septembre, transmis, au département du Trésor des États-Unis, des dizaines de millions de données confidentielles concernant les opérations de ses clients. Un accord Union européenne/États-Unis est signé en juin 2007. Ce dernier autorise la saisie par les États-Unis des données personnelles traitées par Swift aux fins de lutte contre le terrorisme : « Les données de Swift ne sont utilisées que pour extraire des informations concernant une enquête liée au terrorisme précise et en cours. Il en résulte que pour effectuer n'importe quelle recherche, il faut indiquer, éléments de preuve fondés à l'appui, que la personne ciblée par cette recherche a un lien avec le terrorisme ou son financement »[102].

3. — Enfin, l'accord signé entre l'Union européenne et les États-Unis sur le traitement et le transfert des données passagers (Passenger Name Record) par les transporteurs aériens au ministère américain de la sécurité intérieure (US Department of Homeland Security)[103] constitue un autre exemple de transfert de données commerciales à un pays tiers pour des finalités policières. La lettre des États-Unis à l'Union européenne[104] annexée à l'accord précise en son point « I » que : « Le DHS utilise les données PNR de l'U.E. uniquement aux fins :1) de prévenir et de combattre le terrorisme et les délits qui y sont liés; 2) de prévenir et de combattre d'autres délits graves de nature transnationale, y compris la criminalité organisée (...) ». La catégorie visant les traitements de donnée PNR pour « combattre d'autres délits graves », loin de les limiter, étend potentiellement les possibilités de transfert[105]. Par ailleurs, l'accord entre l'Europe et les États-Unis amène à s'interroger : la sécurité intérieure des États-Unis doit-elle être considérée comme une finalité compatible au traitement ultérieur de données commerciales européennes?[106] La question est sans doute un peu provocatrice... mais elle mérite d'être posée, surtout dans la perspective de futurs accords tendant à multiplier les échanges de données à caractère personnel avec ce pays.

Au niveau européen, et depuis 2004[107], les transporteurs aériens ont également l'obligation, sur demande, de communiquer les données API (Advanced Passenger Information) relatives à leurs passagers aux autorités nationales compétentes. Si l'objectif de la mesure vise l'amélioration du contrôle aux frontières et la lutte contre l'immigration clandestine, objectif qui justifiait son adoption dans le cadre du premier pilier, la directive en question s'inscrit indubitablement dans le contexte général de la lutte contre le terrorisme[108]. Pour la Commission, le traitement des données API se révèlent insuffisant, en ce qu'elles « permettent uniquement d'identifier des terroristes et des criminels connus »[109]. C'est la raison pour laquelle une proposition de décision-cadre de 2007 relative à la mise en œuvre d'un système PNR (Passenger Name Record) européen est à l'étude[110]. La valeur ajoutée de cet instrument consisterait à « procéder à des évaluations de risques des personnes, pour obtenir des informations et pour établir des liens entre des personnes connues et des personnes inconnues ». Il n'est plus seulement question d'identifier des terroristes connus, mais de traiter les données PNR à des fins de profilage. L'article 3, § 5, de la proposition prévoit que les données PNR seront traitées dans le but de prévenir ou de combattre les infractions terroristes et la criminalité organisée, en particulier aux fins ci-après : « identifier les personnes qui sont ou qui pourraient être impliquées dans une infraction terroriste ou dans un crime organisé, ainsi que leurs associés; créer et actualiser des indicateurs de risques en vue

présentées par les services répressifs des États membres et Europol à des fins répressives, Bruxelles le 10.09.2009, COM(2009) 344 final, 2009/0130 (CNS), {SEC(2009) 936}, {SEC(2009) 937}.

(99) Créé par la Convention établie sur la base de l'article K3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes du 26 juillet 1995, *J.O.C.E.* C 317, 27 novembre 1995.

(100) Articles 11 et 12 de l'initiative de la république française en vue de l'adoption d'une décision du Conseil relative à la Convention sur l'emploi de l'informatique dans le domaine des douanes (Convention S.I.D.), proposition du 20 janvier 2009, procédure CNS/2009/0803.

(101) P. De Hert et S. Gutwirth, « Interoperability of police databases within the EU : an accountable political choice? », *op. cit.*

(102) Échange de lettres UE/US du 28 juin 2007 concernant Swift, *J.O.C.E.*, 20 juillet 2007, C 166/18 et suivantes. Notez que sous la pression du Parlement européen, le Conseil de l'U.E. a accepté de rouvrir l'an prochain les négociations avec les autorités américaines sur le transfert des données bancaires des citoyens européens. La renégociation pourrait alors être menée selon les règles du Traité de Lisbonne, qui donnent au Parlement la décision finale sur de tels accords. Voy. résolution du Parlement européen du 17 septembre 2009 sur l'accord international envisagé pour mettre à la disposition du département du Trésor des États-Unis des données de messagerie financière afin de prévenir et de combattre le terrorisme et le financement du terrorisme.

(103) Décision 2007/551/PESC/JAI du Conseil du 23 juillet 2007, relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère de la sécurité intérieure (DHS), *J.O.U.E.* L 204, 04/08/2007. Cet accord est le troisième depuis 2004. En effet, un premier accord de 2004, signé dans le cadre du pilier communautaire a fait l'objet d'un arrêt d'annulation par la Cour du Luxembourg, C.J.C.E., 20 mai 2006, *Parlement européen c. Conseil*, aff. C-317/04 et C-318/04 : la Cour considérait alors que l'accord n'était pas fondé sur une base légale appropriée. Un accord provisoire avait ensuite été conclu, avant la signature du troisième accord de 2007.

(104) Traduction de la lettre des États-Unis à l'U.E. publiée au *Journal officiel de l'Union européenne* du 4 août 2007, L 204/21.

(105) Dans ce sens A. Alexandre, « L'échange de données à caractère personnel entre l'Union européenne et les États-Unis », *R.T.D.E.*, juillet-septembre 2006.

(106) La formule nous a été inspirée par le commentaire de Fl. Mariatte à propos de l'arrêt d'annulation par la C.J.C.E. du premier accord PNR : « La sécurité intérieure des États-Unis... ne relève pas des compétences externes des Communautés », *Europe*, juillet 2006, p. 4.

(107) Directive 2004/82/CE concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers aux services de contrôle des frontières, *J.O.U.E.* L 261, 6 août 2004.

(108) Voy. notamment le considérant 2 de la directive 2004/82/CE du 29 avril 2004 faisant référence expresse à la déclaration du Conseil des 25 et 26 mars 2004 sur la lutte contre le terrorisme.

(109) Voy. l'exposé des motifs de la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name record, PNR) à des fins répressives du 6 novembre 2007, COM(2007)654 final.

(110) Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name record, PNR) à des fins répressives, *op. cit.*

d'évaluer ces personnes (...) »[111]. Si le profilage n'est pas en soi un traitement, mais une méthode, au service des finalités traditionnelles poursuivies par les autorités policières, judiciaires ou de sûreté, il n'empêche que cette méthode, déjà partiellement couverte par l'article 15 de la directive 95/46[112] doit être réglementée au vu des risques particuliers que l'utilisation de cette méthode recèle[113]. Ces risques sont liés à la montée en puissance des opérations de *data mining* (multiplication des types de données stockées automatiquement et systématiquement, augmentation de la taille des entrepôts de données et des possibilités d'interconnexion). Étant donnée la complexité des opérations de *data mining*, le risque est grand de voir l'individu pris dans le filet d'une opération de profilage dont la logique ou même l'existence lui échappe : il deviendrait alors incapable d'avoir une quelconque maîtrise sur son image informationnelle ni même de comprendre les mécanismes présidant à la création de cette image, née d'inférences statistiques construites aléatoirement à partir de données qui ne sont pas les siennes[114].

D. — L'érosion du principe de finalité confirmée dans la décision-cadre 977/2008

Last but not least, le dernier point de notre démonstration sur l'érosion du principe de finalité dans l'Espace s'appuie sur les dispositions relatives à ce principe dans la décision-cadre relative à la protection des données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale[115]. En effet, le texte, loin d'assurer un niveau élevé de protection, confirme l'érosion du principe de finalité. Malgré le fait que la décision-cadre rappelle, en son article 3, le principe de finalité déterminée comme suit : « 1. Les données à caractère personnel peuvent être collectées par les autorités compétentes uniquement pour des finalités déterminées, explicites et licites dans le cadre de leurs tâches et traitées uniquement pour les finalités pour lesquelles elles ont été collectées. (...) 2. Le traitement ultérieur pour une autre finalité est permis, dans la mesure où : *a)* ce traitement n'est pas incompatible avec la finalité pour laquelle les données ont été collectées; *b)* les autorités compétentes sont autorisées à traiter ces données pour d'autres finalités conformément aux dispositions légales applicables; et *c)* ce traitement est nécessaire et proportionné à ces finalités. (...) », l'article 11, quant à lui, déroge à ce principe de façon spectaculaire. En effet, il dispose que : « Les données à caractère personnel qui ont été transmises ou mises à dispositions par l'autorité compétente d'un autre État membre peuvent être traitées ultérieurement pour des finalités autres que celles pour lesquelles elles ont été transmises ou mises à disposition dans les cas suivants : *a)* pour la prévention et la détection des infractions pénales, les enquête et les poursuites en la matière ou l'exécution des sanctions pénales; *b)* pour d'autres procédures judiciaires et administratives directement liées à la prévention et à la détection des infractions pénales et poursuite en la matière; c) pour prévenir un danger immédiat et sérieux pour la sécurité publique; *d)* pour toute autre finalité, uniquement avec l'accord préalable de l'État membre qui transmet les données ou avec le consentement de la personne concernée, donné conformément au droit national ». Cette ultime dérogation au principe de traitement ultérieur compatible vient pour ainsi dire vider de sa substance le principe tel que rappelé à l'article 3. La flexibilité de ces dispositions rappelle celle des dispositions de la Convention de 2000 sur l'entraide judiciaire entre États membres[116], qui était alors le premier instrument supranational établissant des règles de protection des données pour les activités judiciaires transnationales[117]. Outre la flexibilité de cette disposition, on reste également perplexe à la lecture de ses conditions d'application, renvoyant à l'accord de l'État membre transmetteur ou au consentement de la personne concernée comme seules limites au traitement ultérieur de données à « toute autre fin ».

E. — La communication de 2004 : renseignement criminel, convergence et stratégie globale d'échanges d'informations entre les autorités policières, douanières et les services de renseignement généraux

Améliorer l'échange d'informations, favoriser le rapprochement opérationnel des services répressifs et mettre en place une stratégie globale d'échange au sein de l'Union européenne sont les actuelles préoccupations de l'Union européenne. Dans sa communication de 2005, la Commission vise en effet « l'introduction d'une action policière et judiciaire fondée sur le renseignement au niveau de l'U.E. (...). Améliorer l'échange d'informations entre toutes les autorités responsables pour le maintien de l'ordre public et pour le respect de la loi, c'est à dire non seulement les forces de police, mais également entre les autorités douanières, les unités de renseignements financiers, l'interaction entre les autorités judiciaires et les services publics de poursuite. (...) Le rôle fondamental que les services nationaux de renseignements et de sécurité jouent à cet égard est incontesté »[118]. Le Conseil précise que le principe de convergence consiste « à favoriser le rapprochement opérationnel des services répressifs des États membres ». Le Conseil souhaite « renforcer la cohérence des dispositifs existants et à venir dans le domaine de la sécurité et favoriser la bonne compréhension par les citoyens européens des politiques menées par l'Union européenne », notamment « en poursuivant l'amélioration des échanges d'informations au sein de l'Union européenne en vue notamment de lutter contre le terrorisme et la criminalité transfrontière » et « en veillant à garantir un niveau élevé de protection des données personnelles dans l'Union européenne »[119].

L'Union européenne devrait donc « mettre en place les cadres juridiques, politiques et opérationnels nécessaires pour veiller à ce que les échanges d'information notamment entre les acteurs légitimes des secteurs publics et privés de l'U.E. puisse se dérouler et soit exécuté de manière de plus en plus efficace »[120].

L'analyse des textes européens, au regard du principe de finalité, fait apparaître des glissements toujours plus importants de traitements aux finalités policières, sans cesse plus divers, de données initialement collectées à des fins déterminées. D'un côté, la notion de finalité compatible est entendue très largement. Cela est dû, d'une part, au principe de disponibilité, qui, conjugué à une interopérabilité croissante des systèmes de données européens, contribue à l'érosion du principe de finalité. On observe

(111) Pour une analyse plus complète de la proposition au regard des principes de protection des données, lire O. De Schutter, T. Ojanen et M. Scheinin, « Thematic legal study : opinion on the draft proposal for a Council framework decision on the use of PNR data for law enforcement purposes », *Fundamental Rights Agency*, 6 octobre 2008.

(112) Sur la méthode de profilage et les insuffisances de l'article 15 à couvrir les risques liés au profilage en général, lire J.-M. Dinant, C. Lazaro, Y. Poullet et A. Rouvroy, rapport au comité consultatif « Convention n° 108 » du Conseil de l'Europe, septembre 2008, disponible sur le site du Conseil de l'Europe. Voy. également, l'excellent ouvrage rassemblant des articles sur le thème du profilage, édité par M. Hildebrandt et S. Gutwirth, *Profiling the European citizen, Cross disciplinary Perspectives*, Springer Science, Dordrecht, Pays Bas, 2008.

(113) L.-A. Bygrave, « Minding the machine : Article 15 of the EC Data Protection directive and Automated Profiling », *Computer Law & Security Report*, 2001, vol. 17, pp. 17-24, disponible en ligne à l'adresse http://www.austlii.edu.au/au/journals/PLPR/2000/40.html.

(114) J.-M. Dinant, C. Lazaro, Y. Poullet et A. Rouvroy, rapport au comité consultatif « Convention n° 108 » du Conseil de l'Europe, *op. cit.*

(115) Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *J.O.U.E.* L 350, 30 décembre 2008.

(116) Acte du Conseil du 29 mai 2000 établissant conformément à l'article 34 du Traité sur l'Union européenne la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union, *J.O.C.E.* C 197, 12 juillet 2000. Son article 23, § 1er, relatif à la « protection des données à caractère personnel » est partiellement comparable à l'article 11 de la décision cadre 2008/977/JAI : « Les données à caractère personnel communiquées au titre de la présente Convention peuvent être utilisées par l'État membre auquel elles ont été transmises : *a)* aux fins des procédures auxquelles la conventin s'applique; *b)* aux fins d'autres procédures judiciaires ou administratives directement liées aux procédures visées au point a); *c)* pour prévenir un danger immédiat et sérieux pour la sécurité publique; *d)* pour toute autre fin, uniquement après consentement préalable de l'État membre qui a transmis les données, sauf si l'État membre concernée a obtenu l'accord de la personne concernée ».

(117) P. De Hert et B. De Schutter, « International Transfers of data in the field of JHA : the lessons of Europol, PNR and Swift », *in Justice, Liberty, Security, new challenges for EU external relations*, VUB-Press, Bruxelles, 2008, pp. 303-339.

(118) Communication de la Commission au Conseil et au Parlement européen du 16 juin 2004, « vers un renforcement de l'accès de l'information par des autorités responsables pour le maintien de l'ordre public et pour le respect de la loi », COM(2004)429 final, non publié au *J.O.*

(119) Conclusion du Conseil sur le principe de convergence et la structuration de la sécurité intérieure du 24 octobre 2008.

(120) Réunion officieuse du comité sur l'article 36 : Paris, 9-10 septembre 2008, annexe au document de séance du Royaume-Uni, « Échange et protection des données dans les domaines de la justice et des affaires intérieures - Éléments clés d'une stratégie d'échange des informations et de protection de données dans les domaines de la justice et des affaires intérieures de l'U.E. ».

aussi un recours croissant des autorités policières aux données collectées par le secteur privé dans le cadre de leurs activités commerciales. De l'autre, la notion de finalité déterminée, dans le domaine policier, perd de sa substance. En effet, l'utilisation des données couvre de plus en plus d'aspects de l'enquête criminelle. Alors qu'à l'origine, les traitements policiers avaient pour finalité la poursuite des infractions pénales déjà commises, cette finalité s'élargit peu à peu aux infractions pénales potentielles, puis au *profiling* en vue du renforcement d'une véritable intelligence criminelle. La question se pose dès lors de savoir comment les notions de finalité déterminée et de traitement ultérieur à des fins compatibles peuvent encore constituer des garanties effectives de protection des données.

4

L'espace de liberté et de sécurité : mais où est la justice ?

L'affaiblissement des règles de protection de données, notamment au travers de l'érosion du principe de finalité, pose nécessairement la question de la conformité des actes européens au regard des droits garantis dans la Convention européenne des droits de l'homme et la Convention 108. Eu égard à la décision-cadre relative à la protection des données dans le troisième pilier, le C.E.P.D. a souligné à plusieurs reprises la faiblesse du niveau de protection offert par rapport à celui requis par la Convention 108[121]. Tel que redouté par le C.E.P.D.[122], le texte de la décision-cadre constitue un compromis basé sur le plus faible dénominateur commun, contenant plusieurs importantes limitations à son champ d'application et multipliant les exceptions[123]. La transposition dans leurs droits nationaux des actes de l'Union pose également un certain nombre de contraintes aux États membres, qui sont tenus tant par l'obligation de coopération loyale envers l'Union[124] que par le respect de l'article 8 de la Convention européenne des droits de l'homme et plus spécialement de la Convention 108, instruments contraignants pour eux. La question de l'articulation des ordres juridiques internationaux, européens et nationaux n'est pas nouvelle. Nous verrons qu'en l'état actuel des traités, le droit de l'Union ne produit que des effets limités (A). La C.J.C.E. n'est pas en mesure d'assurer le contrôle de légalité de ces actes, et par là ne peut garantir une application uniforme du droit de l'Union dans tous les États membres. Au contraire, les juges nationaux et la Convention européenne des droits de l'homme pourraient être conduits à se prononcer sur la légalité des mesures de transposition adoptées par les États membres (B). On sait notamment que la Cour constitutionnelle allemande n'a pas hésité à suspendre en partie l'application des mesures de conservation de données prévues par le *Telekommunikationsgesetz*, jugeant qu'elles étaient incompatibles avec le droit au respect de la vie privée protégée par la Constitution, et invitant par là le législateur à revoir sa copie[125]. Enfin, nous verrons que le Traité de Lisbonne ne fournit que des réponses partielles aux difficultés évoquées (C).

A. — Le droit de l'Union : des effets limités

Pour rappel, les actes du troisième pilier diffèrent dans leur nature et dans leur portée des actes communautaires. Les décisions-cadre et décisions, instruments privilégiés du secteur J.A.I. (justice et affaires intérieures), ont un effet obligatoire à l'égard des États, mais ne peuvent entraîner d'effet direct, contrairement aux actes communautaires du premier pilier qui, à la suite des développements jurisprudentiels de la C.J.C.E., ont acquis cette qualité. Par ailleurs, ces actes sont soumis à un contrôle restreint. Aucune procédure en manquement ne peut être déclenchée par la Commission, tandis que la C.J.C.E. ne bénéficie que d'un contrôle juridictionnel limité. En vertu de l'article 35 U.E., la Cour est compétente pour statuer « à titre préjudiciel sur la validité et l'interprétation des décisions-cadres et des décisions ». La compétence préjudicielle de la Cour étant conditionnée par une déclaration de compétence de la part de chaque État membre[126], la coopération entre les juridictions nationales et la C.J.C.E. dans le troisième pilier est soumise à un régime à géométrie variable[127]. Certains États ne prévoient qu'un renvoi préjudiciel facultatif pour toutes les juridictions[128], d'autres ne prévoient un renvoi obligatoire qu'en dernière instance[129], ou enfin, certains n'ont tout simplement pas fait de déclaration de compétence[130]. En outre, la Cour ne peut exercer son contrôle de légalité direct sur ces actes que sur recours de la Commission et d'un État membre conformément à l'article 35, § 6, ce qui ferme la possibilité au Parlement européen et aux particuliers d'exercer un recours en annulation. L'impossibilité pour le Parlement européen de déclencher un contentieux devant la Cour dans le cadre du troisième pilier est symétrique à son absence dans le processus décisionnel[131], puisque les actes de l'Union sont adoptés à l'unanimité des États réunis au sein du Conseil sans son avis conforme.

Les limites au contrôle juridictionnel de la C.J.C.E. dans le cadre du T.U.E. ne l'ont toutefois pas empêchée de s'appuyer sur des éléments propres à sa jurisprudence pour renforcer l'effectivité du droit de l'Union. Saisie d'un renvoi préjudiciel en interprétation d'une décision-cadre, la Cour a consacré l'obligation d'interprétation conforme du droit national au regard des décisions-cadres[132]. La Cour a étayé son raisonnement sur le caractère contraignant des décisions-cadre, le lien de parenté entre cet instrument et la directive[133] et enfin, sur le principe de coopération loyale énoncé à l'article 10 du T.C.E. Alors qu'il n'apparaissait pas évident que ce principe puisse jouer un rôle semblable dans le cadre du troisième pilier[134], la Cour considère qu'« il serait difficile pour l'Union de remplir efficacement sa mission si le principe de coopération loyale, qui implique notamment que les États membres prennent toutes les mesures générales ou particulières propres à assurer l'exécution de leurs obligations au titre du droit de l'Union européenne, ne s'imposait pas également dans le cadre de la coopération policière et judiciaire en matière pénale »[135]. L'obligation d'interprétation conforme comporte néanmoins une limite. Elle cesse d'exister lorsque le droit national ne peut recevoir une application telle qu'il aboutisse à un résultat compatible avec celui visé par la décision-cadre : « Le principe d'interprétation conforme ne peut donc pas servir à une interprétation *contra legem* du droit national »[136]. Sur l'échelle de l'intensité des effets du droit de l'U.E., la possibilité d'invoquer le besoin d'interprétation conforme est un premier niveau qui vise à garantir aux citoyens une « justiciabilité » minimale[137] du droit de l'Union. Elle ne suffit pas, selon nous, à consacrer la primauté du droit de l'Union sur le droit national, et notamment sur les droits constitu-

(121) Lire deuxième avis du C.E.P.D. du 29 novembre 2006 sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *J.O.U.E.* C 91/9, 26 avril 2007 et troisième avis, *J.O.U.E.* C 139/1, 23 juin 2007.

(122) Voy. troisième avis du C.E.P.D. sur ce texte : « le C.E.P.D. est conscient qu'il est difficile de recueillir l'unanimité au Conseil. Toutefois, la procédure de prise de décision ne saurait justifier une approche favorisant le plus petit dénominateur commun, qui porterait atteinte aux droits fondamentaux ».

(123) D. Alonso Blas, « First pillar and Third pillar : Need for a common approach on data protection? », *Reinventing Data Protection*, *op. cit.*

(124) Ce principe est énoncé à l'article 10 du T.C.E. et a été reconnu dans le cadre du T.U.E. par la C.J.C.E., dans son important arrêt du 16 juin 2005, *Maria Pupino*, aff. C-105/03.

(125) Décision du Bundesverfassungsgericht du 19 mars 2008, 1 BvR 256/08. Lire les commentaires de G. Hornung et Ch. Schnabel, « Data Protection in Germany II : Recent decisions on online-searching of computers, automatic number plate recognition and data retention », *Computer Law & Security Review*, 2009, pp. 115-122. Sur la décision du Bundesverfassungsgericht du 27 février 2008 relative aux perquisitions secrètes en ligne par des agences gouvernementales, lire la note d'observations de P. De Hert, K. De Vries et S. Gutwirth, *R.D.T.I.*, n° 34, 2009, pp. 87-92.

(126) Article 35, §§ 2 et 3, du T.U.E.

(127) O. De Schutter, « Vers l'Union de droit, l'amélioration de la protection juridictionnelle dans l'Union européenne comme élément du débat sur l'avenir de l'Union », rapport final, Cellule de recherche interdisciplinaire en droits de l'homme de l'Université catholique de Louvain, 2003, p. 41.

(128) C'est le cas de la Finlande, de la Grèce, de la Hongrie, de la Lettonie, de la Lituanie, du Portugal et de la Suède.

(129) C'est le cas de l'Allemagne, de l'Autriche, de la Belgique, de l'Espagne de la France, de l'Italie, du Luxembourg, des Pays-Bas, de la république tchèque et de la Slovénie.

(130) C'est le cas du Royaume-Uni, de l'Irlande et du Danemark.

(131) F. Chaltiel, *Le processus de décision dans l'Union européenne*, La Documentation française, Paris, 2006, p. 26.

(132) C.J.C.E., 16 juin 2005, *Maria Pupino*, *op. cit.* L'obligation d'interprétation conforme dans le cadre du pilier communautaire avait quant à elle été reconnue dès 1984 par la Cour : C.J.C.E., 10 avril 1984, *Von Coslon et Kamann*, aff. C-14/83.

(133) Point 34, *Maria Pupino* : « Le caractère contraignant des décisions-cadres, formulé dans des termes identiques à ceux de l'article 249, alinéa 3, CE, entraîne dans le chef des autorités nationales, et en particulier des juridictions nationales, une obligation d'interprétation conforme du droit national ».

(134) M. Fletcher, « Extending « indirect effect » to the third pillar : the significance of *Pupino*? », *European Law Review*, 2005, n° 30, p. 871.

(135) Point 42, *Maria Pupino*.

(136) Point 47, *Maria Pupino*.

(137) Sur l'intensité des effets du droit communautaire, voy. D. Simon, *Le système juridique communautaire*, Paris, P.U.F., 3e éd., 2001, pp. 437-447.

tionnels des États membres, qui sont garants du respect des droits fondamentaux.

B. — Les limites incontournables du système : les risques de mise en cause du droit de l'Union au niveau national et de la C.E.D.H.

1.— L'incomplétude des voies de droit, telle qu'elle résulte du T.U.E., soulève les risques d'une protection disparate des données traitées à des fins répressives. Il ressort de ce système et de la jurisprudence de la C.J.C.E. que, contrairement à ce qu'elle a consacré dans le pilier communautaire, les juridictions nationales pourraient se prononcer directement sur la validité ou non des actes de l'Union au regard des droits fondamentaux, et ceci, afin de garantir une protection juridictionnelle effective aux particuliers[138]. En effet, comme cela a été explicité par l'avocat général Paolo Mendozzi, le régime à la carte de la compétence préjudicielle fondée sur l'article 35 U.E. ne rend pas transposable la règle *Foto-Frost*[139], selon laquelle les juridictions nationales ne sont pas compétentes pour constater directement l'invalidité des actes des institutions communautaires, dans le troisième pilier[140]. Se dessinent ici les limites incontournables du système juridictionnel de l'Union, conduisant l'avocat général à reconnaître que « l'application uniforme du droit de l'Union par les juridictions nationales dans le domaine du troisième pilier de l'Union n'est pas assurée à l'heure actuelle »[141]. Tout recours formé par un particulier contre une mesure nationale qui aurait pour fondement un acte de l'Union pourrait conduire le juge national à se prononcer directement sur la validité de l'acte européen[142]. Ce système soulève des risques de contradiction entre juridictions nationales et, par là, entraîne le risque d'une protection disparate des données à caractère personnel traitées à des fins répressives dans les États membres. On ne peut toutefois que rejoindre la position de l'avocat général selon laquelle « des problèmes bien plus graves résulteraient d'une lecture des dispositions du Traité UE sacrifiant, pour poursuivre vainement l'application uniforme du droit de l'Union dans le domaine du troisième pilier, la protection juridictionnelle des droits qui est inhérente à une communauté de droit »[143].

2. — Enfin, et c'est sans doute le risque majeur qu'encourt le droit de l'Union, l'affaiblissement du niveau de protection des données dans le troisième pilier pourrait générer un contentieux grandissant devant la Convention européenne des droits de l'homme. Il faut d'abord rappeler que les États membres peuvent être tenus responsables devant la Convention européenne des droits de l'homme pour toute mesure de transposition du droit européen, et ceci même s'ils n'usent pas de leur marge d'appréciation. En effet, la Cour strasbourgeoise n'a pas hésité à se prononcer sur la légalité d'une loi française transposant fidèlement une directive[144], rappelant que « les parties contractantes sont responsables au titre de l'article 1er de la Convention de tous les actes et omissions de leurs organes, qu'ils découlent du droit interne ou de la nécessité d'observer des obligations juridiques internationales »[145].

Pour ce qui est de la mise en cause directe du droit de l'Union, toute la difficulté tient évidemment à ce que ni la Communauté, ni l'Union ne soient à ce jour parties à la Convention[146]. Cela avait conduit le juge de Strasbourg à écarter les recours dirigés contre la Communauté faute de compétences *ratione personae* et *loci* établies[147]. Seules les requêtes mettant en cause un État membre ont été jugées recevables[148]. Lorsque dans l'affaire *Bosphorus* concernant l'Irlande, « l'atteinte litigieuse ne procédait pas de l'exercice d'un quelconque pouvoir d'appréciation... mais plutôt du respect par l'État irlandais de ses obligations juridiques résultant du droit communautaire », la Cour a avancé la doctrine très controversée de présomption de compatibilité du droit communautaire à la Convention. Dans une formule consistant à réconcilier les ordres juridiques nationaux et européens, la Cour jugeait que la Communauté « offre une protection à tout le moins équivalente à celle assurée par la Convention »[149]. La présomption de compatibilité du droit communautaire à la Convention européenne des droits de l'homme n'est pas irréfragable : « pareille présomption peut toutefois être renversée dans le cadre d'une affaire donnée si [...] la protection des droits garantis par la Convention est entachée d'une insuffisance manifeste »[150]. L'arrêt *Bosphorus* a fait l'objet de nombreux commentaires[151]. Aussi, notre propos se limitera ici à en rappeler quelques-uns. Dans leur opinion prétendument concordante, pas moins de six juges ont souligné le risque d'un double standard de protection, dans la mesure où l'approche *Bosphorus* revient à exempter certains États d'un examen de conformité de leurs actes, tandis que d'autres y sont toujours exposés[152]. Des doutes sérieux ont aussi été émis quant au raisonnement théorique et abstrait fondé sur les mécanismes de contrôle de la C.J.C.E., qui a conduit à la conclusion d'équivalence de protection. Pour ces mêmes juges, la proportionnalité d'une mesure (question qui était posée à la Cour en l'espèce) ne pouvait être examinée qu'*in concreto*, tandis que la majorité s'était livré à un examen général et *in abstracto* du système communautaire. Le juge Ress, quant à lui, avait tenu à souligner l'éventuelle « insuffisance manifeste » de protection des droits garantis dans l'article 6, § 1er, de la Convention euro-

(138) La problématique du droit à une protection juridictionnelle effective a été particulièrement révélée par le contentieux de l'inscription sur des listes d'organisations terroristes. Ces affaires posaient notamment la question de la conformité d'actes adoptés sur les fondements des deuxième et troisième piliers au regard des droits fondamentaux. Voy. notamment C.J.C.E., 27 février 2007, *SEGI c. Conseil*, aff. C-355/04 et *Gestoras Pro Amnistia c. Conseil*, aff. C-354/04. À ce sujet, lire le commentaire de S. Marciali, « Le droit à un recours effectif en droit de l'Union européenne : quelques progrès, beaucoup d'ambiguïtés », *R.T.D.H.*, 2007, pp. 1154-1170.

(139) C.J.C.E., 22 octobre 1987, *Foto-Frost*, aff. C-314/85, *Rec.*, p. 4199. La règle Foto-Frost, selon laquelle les juridictions nationales ne sont pas compétentes pour constater directement l'invalidité des actes des institutions communautaires, a été posée dans le pilier communautaire en vue de garantir une application uniforme du droit communautaire dans tous les États membres.

(140) Point 112 à 127 des conclusions de M. l'avocat général Paolo Mendozzi, 26 octobre 2006, *Gestoras*.

(141) Point 130 des conclusions de M. l'avocat général Paolo Mendozzi, *Gestoras*.

(142) L'article 35 U.E. ne fait référence qu'à la « faculté » et non à « l'obligation » pour les juridictions nationales de saisir la Cour, contrairement à l'article 234 CE qui prévoit que toute juridiction statuant en dernier ressort « est tenue » de saisir la C.J.C.E. Conformément à la déclaration n° 10 annexée au Traité d'Amsterdam, certains États ont cependant prévu un renvoi obligatoire en dernière instance. Dans sa jurisprudence *Gestoras* du 27 février 2007, la Cour semble s'en tenir à la « faculté » pour les juridictions nationales de saisir la Cour d'un renvoi préjudiciel quand la validité d'une mesure nationale prise sur le fondement d'un acte de l'Union serait contestée devant elles.

(143) Point 130 des conclusions de M. l'avocat général Paolo Mendozzi, *Gestoras*.

(144) C.E.D.H., *Cantoni c. France*, 15 novembre 1996.

(145) Ce qu'elle a jugé dans C.E.D.H., *Parti communiste unifié de Turquie et autres c. Turquie*, 30 janvier 1998, § 29.

(146) La compétence de la C.J.C.E. avait été sollicitée sur la question de l'adhésion de la Communauté à la Convention européenne des droits de l'homme. Dans son avis du 28 mars 1996, la C.J.C.E. avait alors considéré que la Communauté n'avait pas, en l'état actuel des traités, compétence pour adhérer à la C.E.D.H., C.J.C.E., avis n° 2/94, 28 mars 1996, *Rec.*, I, p. 1759. Lire notamment les commentaires de V. Constantinesco, note sous Cour de justice des Communautés européennes (C.J.C.E.), 28 mars 1996, avis 2/94, *Journal du droit international*, 1997, n° 2, p. 519 et P. Wachsmann, « L'avis 2/94 de la Cour de justice relatif à l'adhésion de la Communauté européenne à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales », *R.T.D. eur.*, 1996, n° 3, p. 490. La question subsiste : la C.J.C.E. n'adopterait-elle pas un avis cette fois favorable depuis l'insertion par le Traité d'Amsterdam de l'article 6 du T.C.E. faisant référence expresse au respect des droits fondamentaux et aux compétences de la Communauté en la matière?

(147) Il s'agit d'une jurisprudence constante depuis C.E.D.H., aff. *CFDT c. Communautés européennes*, 10 juillet 1978, rappelé dans C.E.D.H., aff. *Dufay c. Communautés européennes*, 19 janvier 1989.

(148) L'ancienne Commission et la Cour ont en effet jugé recevable une requête mettant en cause un État membre pour un acte de droit primaire. Voy. C.E.D.H., aff. *Matthews c. Royaume-Uni*, 18 février 1999. Le Royaume-Uni avait été condamné pour violation de l'article 3 du protocole n° 1 à la Convention qui prévoit l'organisation d'élections libres au scrutin secret, jugeant ainsi contraire à la Convention l'annexe excluant Gibraltar du champ d'application de l'acte de 1976 relatif à l'élection du Parlement européen au suffrage universel direct. Elle a également jugé recevables les requêtes dirigées contre un État membre concernant des actes nationaux pris en application du droit communautaire dérivé, comme dans l'affaire *Cantoni*.

(149) C.E.D.H., aff. *Bosphorus c. Irlande*, 30 juin 2005, § 148.

(150) *Bosphorus*, § 156.

(151) Lire notamment, F. Benoit-Rohmer, « À propos de l'arrêt Bosphorus Airlines du 30 juin 2005 : l'adhésion contrainte de l'Union à la Convention », *R.T.D.H.*, 2005, n° 46, p. 827; V. Constantinesco, « C'est comme si c'était fait? », (observations à propos de l'arrêt de la C.E.D.H., gde ch., *Bosphorus Airlines*, du 30 juin 2005), *Cahiers de droit européen*, 2006, n° 3-4, pp. 363-378; C. Eckes, « Does the European Court of Human Rights provide protection from the European Community? », *European Public Law Review*, vol. 13, issue 1, février 2007, p. 47; J.-P. Jacque, « L'arrêt *Bosphorus*, une jurisprudence "Solange II" de la Cour européenne des droits de l'homme? », *R.T.D. eur.*, juillet-septembre 2005, p. 756, F. Kauff-Gazin, « L'arrêt *Bosphorus* de la C.E.D.H. : quand le juge de Strasbourg décerne au système communautaire un label de protection satisfaisante », *Petites Affiches*, 24 novembre 2005, n° 234, p. 14; K. Kuhnert, « *Bosphorus* - Double standards in European rights protection? », *Utrecht Law Review*, vol. 2, issue 2, décembre 2006, disponible sur http://utrechtlawreview.org/, M. Melchior, « L'arrêt *Bosphorus c. Irlande* de la Cour européenne des droits de l'homme du 30 juin 2005 : un arrêt étrange au sujet de la relation entre droit communautaire et droit de la Convention européenne des droits de l'homme », *Revue de la Faculté de droit de l'Université de Liège*, vol. 1-2, 2006, pp. 245-255; F. Sudre, « La "conventionnalité" du système communautaire de protection des droits fondamentaux », *J.C.P.*, G, semaine juridique, 2005, n° 39, p. 1760.

(152) Opinion concordante commune à l'arrêt *Bosphorus* des juges Rozakis, Tulkens, Traja, Botoucharova, Zagrebelsky et Garlicki. Sur cette question, lire notamment K. Kuhnert, « *Bosphorus* - Double standards in European rights protection? », *op. cit.*

péenne des droits de l'homme en raison de l'accès restreint des particuliers à la C.J.C.E., précisément dans le cadre des deuxième et troisième piliers[153]. La théorie de l'équivalence de protection a parfois été interprétée comme une immunité du droit communautaire devant la Convention européenne des droits de l'homme dans la mesure où la preuve d'une insuffisance manifeste, et non celle d'une simple violation des droits garantis serait nécessaire pour écarter cette présomption[154]. À l'opposé, d'autres ont évoqué une « adhésion contrainte » de l'U.E. à la Convention européenne des droits de l'homme, s'appuyant sur le fait que *Bosphorus* ouvrait enfin la voie au contrôle des actes communautaires par la Cour de Strasbourg[155]. Selon nous, la solution retenue s'analyse aussi comme une étape intermédiaire à l'adhésion, une solution provisoire de conciliation des ordres juridiques. Ici encore, se dessinent les limites du système. Dans la mesure où l'espace de liberté et sécurité, cher à l'Union, vise également à être un espace de justice, l'adhésion de l'Union à la Convention nous semble un élément indispensable à cet objectif.

C. — Quelles évolutions possibles ? Le Traité de Lisbonne

Comme il est coutume de le rappeler, l'entrée en vigueur du Traité de Lisbonne marque une nouvelle étape dans le processus d'intégration européenne. Parmi les modifications apportées aux traités actuels, on relève bien sûr la « dépillarisation » du système. Dans ce cadre, l'Union se substitue et succède à la Communauté, attribuant la même valeur juridique au futur traité sur l'U.E. (T.U.E.) et traité sur le fonctionnement de l'U.E. (T.F.U.E.)[156]. La protection des données à caractère personnel fait désormais explicitement partie des compétences de l'Union, puisqu'elle s'est vu octroyer une base juridique unique dans le futur T.F.U.E.[157]. Toutefois, nous verrons qu'en ce qui la concerne, la disparition des piliers n'est qu'apparente (1). Enfin, parmi les modifications des traités actuels qui nous intéressent, il faut bien sûr relever l'entrée en vigueur de la Charte des droits fondamentaux de l'Union européenne et l'adhésion de l'Union à la Convention européenne des droits de l'homme (2).

1. — *Le principe d'un cadre légal de protection des données par « piliers » non remis en question*

Conséquence de la suppression des piliers, la protection des données à caractère personnel est dotée d'une base juridique unique pour les matières relevant des premier et troisième piliers. L'article 16 T.F.U.E. reconnaît que « toute personne a droit à la protection des données personnelles la concernant. » Le paragraphe 2 prévoit notamment que « le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données ». Le progrès essentiel réside dans la dépillarisation procédurale et contentieuse. Toute mesure relative à la protection des données sera adoptée par le Parlement et le Conseil en codécision, devenue la procédure législative ordinaire[158]. Le règne de l'unanimité dans le troisième pilier est donc abandonné. On est permis d'espérer en amont un plus grand contrôle du Parlement européen sur les actes adoptés dans le cadre de l'E.L.S.J. En référence à nos développements précédents, il faut aussi souligner que tous les actes seront désormais soumis au contrôle juridictionnel de la Cour dans les conditions semblables à celles que prévoit le T.C.E.[159]. Il s'agit là d'un progrès fondamental eu égard à l'objectif de réalisation d'une « Union de droit », où « ni ses États membres, ni ses institutions n'échappent au contrôle de conformité de leurs actes à la charte constitutionnelle de base qu'est le Traité »[160]. D'un point de vue substantiel, plusieurs remarques s'imposent. Le champ des compétences de l'Union en ce domaine n'est pas sensiblement élargi. En premier lieu, la compétence de l'Union à réguler les traitements de données réalisés par ses institutions et organes constitue une reprise de l'article 286 CE. En second lieu, sa compétence à réguler les traitements de données réalisés dans les États membres est limitée aux « activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données ». C'est donc un encadrement de la compétence par la compétence de l'Union à agir dans certains domaines. Il faut alors lier cette base unique de l'article 16 à la répartition des compétences consacrée aux articles 2 à 6 du T.F.U.E. En effet, le Traité de Lisbonne établit une typologie tripartite des compétences, fondée tant sur la jurisprudence que sur la pratique. Cette typologie consiste à distinguer les compétences exclusives, partagées, et celles dites d'appui de coordination ou de complément[161]. Les domaines de compétence du marché intérieur et de l'Espace de liberté, sécurité et justice, compétences sur lesquelles se sont fondés l'adoption de règles relatives à la protection des données, font explicitement partie des compétences partagées entre l'Union et les États membres[162]. La protection des données continuera donc elle aussi de relever du champ des compétences partagées. Enfin, la base unique de l'article 16 ne s'oppose pas à ce que le législateur européen prévoie des règles particulières de protection des données en matière de coopération policière et judiciaire et plus généralement de sécurité nationale. C'est ce que les déclarations n^{os} 20 et 21 annexées au Traité invitent même à faire, prévoyant respectivement que « chaque fois que doivent être adoptées, sur la base de l'article 16, des règles[...] qui pourraient avoir une incidence directe sur la sécurité nationale, il devra en être dûment tenu compte »[163], tandis que « des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation de ces données dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière se basant sur l'article 16 du T.F.U.E. pourraient s'avérer nécessaires »[164]. Le principe d'une protection des données à caractère personnel distincte selon le domaine de compétence semble désormais établi. En d'autres termes, la coexistence des instruments actuels, directive 95/46 et décision-cadre 977/2008 ne sera pas remise en question nonobstant la consécration d'une base unique[165]. Il s'agit là en quelque sorte d'une survivance du système en piliers qui a contribué à la fragmentation du cadre légal européen de protection des données selon que l'on se situe dans la sphère commerciale ou dans la sphère répressive. Au sein même de la sphère répressive, le cadre légal de la protection des données personnelles sera par ailleurs divisé entre la coopération policière et judiciaire en matière pénale et la P.E.S.C., complexifiant encore le système.

Si elle constitue une avancée, en ce sens qu'elle ouvre la voie à une régulation des traitements de données dans le cadre de la P.E.S.C., la base juridique de l'article 39 du T.U.E. constitue un autre exemple de la survivance des piliers en matière de protection des données. Il prévoit que par dérogation à l'article 16, § 2, du T.F.U.E. le Conseil adopte une décision fixant les règles relatives à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par les États membres dans

(153) Dans son opinion concordante, le juge Ress considère qu'il y a insuffisance manifeste de protection « lorsque, du point de vue procédural, il n'y a pas eu de contrôle adéquat dans l'affaire considéré, par exemple, lorsque la C.J.C.E. n'est pas compétente », se référant à titre d'exemple à l'affaire *Gestoras*, qui était, au moment de Bosphorus, pendante devant la C.J.C.E.. L'affaire *Gestoras* visait alors un recours en indemnité introduit du fait du préjudice subi par une position commune, prise sur les fondements des deuxième et troisième piliers.

(154) L.F.M. Besselink, « The European Union and the European Convention on Human Rights after the Lisbon Treaty : from *Bosphorus* sovereign immunity to full scrutiny? », available on http://ssrn.com.

(155) F. Benoit-Rohmer, « À propos de l'arrêt *Bosphorus Airlines* du 30 juin 2005 : l'adhésion contrainte de l'Union à la Convention », *op. cit.*

(156) Article 1er du futur T.U.E.

(157) Pour un commentaire général de l'article 16 du futur T.F.U.E., voy. F.-X. Priollaud et D. Siritzky, *Le Traité de Lisbonne, texte et commentaire article par article des nouveaux traités européens (T.U.E.-T.F.U.E.)*, La Documentation française, Paris, 2008, pp. 172-174.

(158) Article 294 du T.F.U.E., actuel article 251 du T.C.E.

(159) Le recours en annulation (article 263 du T.F.U.E., actuel article 230 du T.C.E.), la procédure de renvoi préjudiciel (article 267 du T.F.U.E., actuel 234 du T.C.E.), le recours en indemnité (articles 268 et 340 du T.F.U.E., actuel articles 235 et 288, § 2) ainsi que le recours en carence (article 265 du T.F.U.E. et 232 du T.C.E.) seront applicables aux actes adoptés dans le cadre de l'E.L.S.J. La dérogation prévue à l'actuel 35, § 5, du T.U.E. est maintenu à l'article 276 du T.F.U.E. : « la Cour de justice n'est pas compétente pour vérifier la validité ou la proportionnalité d'opérations menées par la police ou d'autres services répressifs dans un État membre, ni pour statuer sur l'exercice des responsabilités qui incombent aux États membres pour le maintien de l'ordre public et la sauvegarde de la sécurité intérieure ».

(160) C.J.C.E., 23 avril 1986, *Parti écologiste « Les Verts » c. Parlement européen*, aff. C-294/83, point 23. Pour une analyse approfondie des perspectives et changements relatifs au contrôle juridictionnel de la C.J.C.E., voy. A. Weyemberg et V. Ricci, « Le Traité de Lisbonne et le contrôle juridictionnel sur le droit pénal de l'Union européenne », *in Le contrôle juridictionnel dans l'Espace pénal européen*, Université de Bruxelles, 2009.

(161) Voy. notamment J.-P. Jacque, « Le Traité de Lisbonne, une vue cavalière », *R.T.D. eur.*, n^{o} 44, juillet-septembre 2008, pp. 472-478.

(162) Voy. la liste non exhaustive des domaines de compétences partagées à l'article 4, § 2, du T.F.U.E.

(163) Déclaration *ad* article 16 du T.F.U.E., n^{o} 20.

(164) Déclaration sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, n^{o} 21.

(165) Dans le même sens voy. D. Alonso Blas, « First pillar and Third pillar : Need for a common approach on data protection? », *Reinventing Data Protection*, *op. cit.*

l'exercice de la P.E.S.C. et à la libre circulation de ces données. Le pilier P.E.S.C. devrait donc lui aussi être doté de son propre instrument. Les traités prévoient que les décisions relevant de la P.E.S.C. sont prises par le Conseil européen et le Conseil à l'unanimité[166]. Contrairement à ce qui est prévu dans les autres domaines, ces décisions ne seront pas des actes législatifs[167]. Autre conséquence de leur régime spécifique, les actes de la P.E.S.C., sauf exception, échapperont au contrôle juridictionnel de la C.J.C.E.[168].

2. — *Les avancées : un cadre légal écrit et exhaustif de protection des droits fondamentaux*

Le cadre légal européen de la protection des données semble confirmer le principe d'une protection différenciée, selon le domaine dans lequel l'Union agit. En revanche quelles que soient les spécificités, l'Union sera tenue du respect de la Charte des droits fondamentaux et de la Convention européenne des droits de l'homme. Cette obligation de respect constitue la clarification la plus importante apportée par le Traité de Lisbonne, qui établit dorénavant un système écrit de protection des droits fondamentaux[169]. Bien qu'elle ne figure plus directement dans les traités, comme prévu au départ par le projet avorté de Constitution, la Charte des droits fondamentaux acquiert une valeur juridique contraignante et accède au rang de source de droit primaire[170]. La portée de la Charte et de son champ d'application y sont clairement définis. L'article 51 prévoit qu'elle s'adresse aux « institutions, organes et organismes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union. » Les institutions européennes, au sens large, sont donc soumises au respect de la Charte, quel que soit le pilier[171]. En ce qui concerne les États membres, la Charte ne s'applique pas aux activités nationales qui se situent dans le champ des compétences nationales. La possibilité pour les individus d'invoquer la Charte est ordonnée autour de la distinction entre droits et principes. Tandis que les droits garantis par la Charte seraient toujours justiciables à l'encontre d'une mesure de l'Union ou d'une mesure nationale d'application, les individus ne pourraient se prévaloir directement de la violation d'un principe. Si la Charte ne dit rien sur les dispositions qui garantissent des droits et celles qui garantissent des principes, nul doute que le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, reconnus respectivement aux articles 7 et 8, se rangent dans la catégorie des droits directement justiciables par les individus[172]. Enfin, le futur dispositif de protection des droits fondamentaux sera complété par l'adhésion de l'Union européenne à la Convention européenne des droits de l'homme. Le juge de Luxembourg sera tenu d'appliquer directement la Convention, et de reprendre la jurisprudence de la Cour européenne des droits de l'homme pour les droits dont le sens et la portée sont les mêmes que dans la Charte. Le *dialogue des juges* luxembourgeois et strasbourgeois sera alors une composante essentielle au perfectionnement du système de protection des droits fondamentaux, afin d'éviter toute contradiction entre la C.J.C.E. et la Cour européenne des droits de l'homme. L'Union européenne pourra être directement justiciable devant la Cour européenne des droits de l'homme pour tous les actes qui produiraient des effets de droit sur les individus. Sa responsabilité pourra alors être recherchée indépendamment de celles des États membres, tandis que les inconvénients actuels de la jurisprudence *Bosphorus* seront dissipés. L'entrée en vigueur du Traité de Lisbonne offre les outils d'une protection des droits fondamentaux plus aboutie au niveau de l'Union, en remédiant aux insuffisances du contrôle juridictionnel de l'Union et en assurant une meilleure articulation des systèmes.

5 Conclusion

Notre conclusion est sévère. L'introduction relevait les principes de protection des données mis en avant par la jurisprudence du Conseil de l'Europe. Au terme de notre analyse, nous relevons que nombre de ces principes ne sont pas rencontrés par les textes de l'Union européenne analysés. Ceux-ci pêchent par l'absence de précision des finalités poursuivies par les traitements de données collectées, oublient volontiers les précautions à prendre en matière de profilage et de décisions automatisées et négligent le contrôle de proportionnalité que pourraient offrir les instances parlementaires.

Les faiblesses rencontrées dans les textes analysés résultent d'une vision européenne très particulière de la manière dont doit s'opérer l'articulation entre les libertés et les impératifs de sécurité. Le récent programme de travail de Stockholm[173] est illustratif de ce propos. Tout d'abord, le concept européen de « sécurité », englobant « trois domaines d'action complémentaires et désormais indissociables : le renforcement de la coopération policière, une justice pénale adaptée et une gestion de l'accès au territoire plus efficace »[174], semble confondre lutte contre le terrorisme, répression de la criminalité et gestion de l'immigration, devenant ainsi peu à peu un « conteneur » général justifiant des atteintes aux libertés pour des finalités éparses et traditionnellement distinguées entre elles. Ensuite, pour faire face à ce défi sécuritaire global, les autorités de l'Union prônent « une véritable architecture des systèmes d'information en tirant profit des expériences acquises. Celle-ci assurera l'interopérabilité des solutions techniques retenues au niveau national et des systèmes européens existants ou à venir »[175]. Un modèle technologique global pour répondre à un défi sécuritaire global, tel semble être le plan d'action prôné par le programme de Stockholm pour les cinq années à venir. En effet, selon celui-ci, « la sécurité dans l'Union repose sur des mécanismes performants d'échanges d'informations entre les autorités nationales et les acteurs européens. À cette fin, l'Union doit se doter d'un modèle européen d'information fondé à la fois sur un renforcement de la capacité d'analyse stratégique et sur l'amélioration de la collecte et du traitement des informations opérationnelles. Ce modèle doit tenir compte des cadres existants, y compris dans le domaine douanier, et permettre de relever les défis liés à l'échange d'information avec les pays tiers »[176]. De plus, « l'Union doit renforcer considérablement sa capacité d'analyse et de synthèse des informations stratégiques dont elle dispose. À cet égard, les synergies entre Europol et Frontex doivent être améliorées »[177].

Alors que la stratégie sécuritaire européenne est caractérisée par la volonté de mettre en place un modèle européen transversal d'informations, le principe de base de la protection des données impose de ne traiter des données à caractère personnel que pour des finalités déterminées et compatibles. Toute la difficulté de l'articulation entre sécurité et liberté découle de ces objectifs discordants : globalisation d'un côté, segmentation par finalité de l'autre. En résulte l'érosion lente du principe de finalité constatée à travers les textes analysés.

Il est donc permis de douter sérieusement de la réalisation de l'objectif visant à garantir un haut niveau de protection des données dans l'espace de liberté, de sécurité et de justice. La décision-cadre du troisième pilier apparaît davantage comme un consensus faible où les États membres n'ont su se rejoindre que sur le plus petit dénominateur commun. La décision-cadre n'apporte pas de valeur ajoutée au système de protection des données, mais plutôt offre des opportunités aux États membres de déroger à certains de ses principes fondamentaux, en même temps qu'il contient des dérogations importantes aux principes de la Convention européenne des droits de l'homme qui avaient pourtant été traduits correctement dans le premier pilier. La marge d'appréciation laissée aux États membres dans la mise en œuvre du droit de l'Union, mais aussi les risques de mise en cause de ces mesures nationales devant le juge natio-

(166) Article 24 du futur T.U.E.

(167) Il est précisé à deux reprises, aux articles 24 et 31 du T.U.E. relatifs à la P.E.S.C. que « l'adoption d'actes législatifs est exclue ».

(168) Article 24 du futur T.U.E. et 275 du T.F.U.E.

(169) J.-P. Jacque, « Le Traité de Lisbonne, une vue cavalière », *R.T.D. eur.*, n° 44, juillet-septembre 2008, pp. 472-478.

(170) Article 6, § 1er, du T.U.E.

(171) Nous conservons ici volontairement l'expression au vu de nos développements précédents relatifs à la P.E.S.C. et à la confirmation d'un cadre légal fragmenté de protection des données entre le domaine commercial et répressif

(172) D'un côté, le droit au respect de la vie privée tel que consacré dans la Charte constitue un droit dont le sens et la portée sont les mêmes que dans la Convention européenne des droits de l'homme. De l'autre, la protection des données à caractère personnel, prolongement de la vie privée, est aussi expressément reconnue dans le T.F.U.E., article 16.

(173) Conjointement avec la présidence suédoise du Conseil européen, la Commission a présenté un programme d'envergure pour les cinq prochaines années visant à développer un espace de liberté, de sécurité et de justice au service des citoyens. Il a été surnommé le « programme de Stockholm » et doit être adopté par le Conseil européen du 10 décembre 2009. Il fait suite aux programmes antérieurs couvrant une période de cinq ans dans les mêmes domaines d'action, à savoir le programme de La Haye et le programme de Tampere. Voy. communication de la Commission au Parlement européen et au Conseil, 10 juin 2009, COM (2009) 262/4.

(174) *Ibidem*, p. 17.

(175) *Ibidem*, p. 16.

(176) *Ibidem*, p. 15.

(177) *Ibidem*.

nal ou la Cour européenne des droits de l'homme accentuent encore le risque d'un manque d'harmonisation.

Le Traité de Lisbonne devrait permettre de remédier en partie à ces difficultés. Parmi les avancées importantes, on note le plus grand contrôle de légalité des actes adoptés dans le cadre de l'Espace. Le volet « justice » de l'espace de liberté et de sécurité devrait être considérablement renforcé par le futur traité. Il constitue aussi une amélioration importante quant au déficit démocratique dont souffre l'adoption des actes du troisième pilier, et ce par la généralisation de la procédure de codécision. Toutefois, pour ce qui concerne la protection des données, le principe d'un cadre légal différencié selon que l'on se situe dans la sphère « marché intérieur » ou celle « justice, libertés et sécurité » ne sera pas remis en question.

Enfin, nous espérons qu'à l'avenir le principe de finalité sera pleinement respecté au sein de l'Espace dit J.L.S., conformément à l'engagement du programme de Stockholm selon lequel « l'espace de liberté, de sécurité et de justice doit être avant tout un espace unique de protection des droits fondamentaux, au sein duquel le respect de la personne et de la dignité humaine ainsi que des autres droits consacrés dans la Charte des droits fondamentaux constitue une valeur essentielle. Il s'agit par exemple de préserver l'exercice de ces libertés et la sphère privée du citoyen au-delà des frontières nationales, notamment via la protection de ses données personnelles »[178]. Ce n'est que de cette manière que les autorités européennes pourront réellement mettre l'espace de liberté, de sécurité et de justice « au service des citoyens » et de leurs droits.

F. DUMORTIER[179]
C. GAYREL[180]
J. JOURET[181]
D. MOREAU[182]
et Y. POULLET[183]

(178) *Ibidem*, p. 5.

(179) F. Dumortier est assistant en droit aux F.U.N.D.P. (Namur) et chercheur senior au C.R.I.D. (Centre de recherches informatique et droit), unité « libertés dans la société de l'information ».

(180) C. Gayrel est chercheuse en droit au C.R.I.D. (Centre de recherches informatique et droit), unité « libertés dans la société de l'information ».

(181) J. Jouret est attachée au S.P.F. Justice, direction générale de la législation et des libertés fondamentales, service des droits de l'homme, cellule vie privée. Écrit en son nom personnel.

(182) D. Moreau est attaché au S.P.F. Justice, direction générale de la législation et des libertés fondamentales, service des droits de l'homme, cellule vie privée. Écrit en son nom personnel.

(183) Y. Poullet est professeur en droit aux F.U.N.D.P. et directeur du C.R.I.D. (Centre de recherches informatique et droit).

Arrêt « Glaxosmith » : les clauses contractuelles relatives au commerce parallèle des médicaments

LES CLAUSES limitant, d'une manière ou d'une autre, la possibilité, pour un revendeur, d'exporter des médicaments vers d'autres États membres, où les prix de vente sont plus élevés, sont-elles conformes à l'interdiction des restrictions contractuelles anticompétitives (article 101 T.F.U.E.)?

1 Introduction

Le 6 octobre 2009, la Cour de justice s'est prononcée dans l'affaire *Glaxo-Espagne*[1]. Il s'agissait de l'un des arrêts des plus attendus de l'année. Il concernait en effet une affaire entamée dès 1998 avec la notification, par Glaxo, de ses nouvelles conditions de ventes à la Commission. En outre, cet arrêt était également fortement attendu étant donné qu'il concernait l'application de l'article 101 T.F.U.E. (ex article 81 CE) au secteur pharmaceutique[2].

À cet égard, l'arrêt de la Cour de justice ferme la porte que l'arrêt du Tribunal du 27 septembre 2006 avait ouverte[3]. Un autre arrêt a été rendu récemment par la Cour, à propos de la même entreprise, et concernant des pratiques ayant une objet analogue[4]. Cet arrêt est fondé sur l'article 102 T.F.U.E. Nous ne discuterons pas, dans le commentaire, de la relation entre ces arrêts. Un article plus global sera consacré à cette question ultérieurement.

Dans la présente affaire, quelle solution la Cour a-t-elle retenue? La Cour de justice a rejeté l'ensemble des pourvois qui avaient été formés. En terme de résultats, la décision de la Commission du 8 mai 2001 reste en vigueur. Il en résulte que le système de prix double de Glaxo enfreint l'article 101, § 1er, T.F.U.E. et ne peut être sauvé au regard de l'article 101, § 3, T.F.U.E.

Il est important de relever que la Cour a fait basculer la balance du côté du point de vue strict adopté par la Commission. Le signal est clair : les restrictions du commerce parallèle enfreignent l'article 101, § 1er, T.F.U.E. par objet, dans le secteur pharmaceutique à l'instar de tout autre secteur économique. Reste toutefois en suspens la question de savoir si de telles restrictions peuvent satisfaire aux conditions d'une exemption, même si cette voie s'annonce d'ores et déjà difficile.

2 Les faits

Glaxo a notifié à la Commission ses nouvelles conditions générales de vente destinées à ses grossistes espagnols. L'article 4 de ces conditions prévoyait deux niveaux de prix de vente : un prix bas pour tous les produits assujettis aux règles de remboursement en Espagne (donc les produits revendus aux hôpitaux et pharmacies en Espagne), et un prix supérieur pour tous les cas où les grossistes fixent librement leur prix.

La logique paraît limpide : si les grossistes fixent les prix de revente librement, Glaxo doit être en mesure de fixer son prix de vente selon des critères économiques réels, objectifs et non discriminatoires. Par contre, dans les cas où les grossistes sont tenus par les prix particulièrement bas fixés par les autorités nationales en Espagne, Glaxo permet aux grossistes de faire une marge acceptable en appliquant un prix de vente adapté. Une logique qui ne traduit aucunement une intention de vouloir saboter l'intégration du marché commun ou de faire payer les consommateurs des prix artificiellement gonflés. Hélas, aux yeux de la Commission, il découle de cet article 4 que les prix bas s'appliquent uniquement aux produits vendus en Espagne. L'article 4 empêcherait donc, selon elle, les grossistes espagnols d'acheter au prix bas pour l'exportation. S'ils exportent des médicaments, ils doivent en effet payer le prix plus élevé.

(1) C.J., 6 octobre 2009, *GlaxoSmithKline Services e.a. c. Commission e.a.*, aff. jtes C-501/06P, C-513/06 P, C-515/06 P et 519/06 P, non encore publié au *Recueil*.

(2) C. Hatton, A. Bicarregui et D. Cardwell, « "Interesting times" for pharmaceutical companies : European competition law and the pharmaceutical sector » *in* G. Michaux (éd.), « Consommateurs, médicaments et industrie pharmaceutique », *R.E.D.C.*, 2009/2, p. 381.

(3) Trib., 27 septembre 2006, *GlaxoSmithKline Services c. Commission*, T-168/01, *Rec.*, 2006, p. II-2969.

(4) C.J., 16 septembre 2008, *Sot. Lélos kai Sia*, aff. jtes. C-468/06 à C-478/06, *Rec.*, 2008, p. I-7139; voy., à cet égard, D. Waelbroeck et J.-F. Diaz, « Commerce parallèle et produits pharmaceutiques - Premières leçons des deux arrêts "Glaxo" », *J.D.E.*, 2008, p. 269. C. Chenevière, « Médicaments, exportations parallèles et abus de position dominante, », *R.E.D.C.*, 2007-2008/3, p. 425.